European Union Agency for Network and Information Security

DECISION No MB/2019/3 of the Management Board of the European Union Agency for Network and Information Security (ENISA) amending the Programming Document 2019-2021 and Statement of estimates 2019

THE MANAGEMENT BOARD OF ENISA,

Having regard to Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, and in particular articles 13 and 19 thereof;

Having regard to the Decision No MB/2014/1 WP of the Management Board of the European Union Agency for Network and Information Security (ENISA) on the financial regulation applicable to the European Union Agency for Network and Information Security in conformity with the Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council, and in particular article 33(8);

Having regard to Commission Communication C(2014) 9641 final, on the guidelines for programming document for decentralised agencies and the template for the Consolidated Annual Activity Report for decentralised agencies dated 16.12.2014;

Having regard to the General budget 2019 of the European Union, in particular Section III[1];

Having regard to the decision No MB/2018/20 of the Management Board of the European Union Agency for Network and Information Security (ENISA) adopting the Programming Document 2019-2021, the Statement of estimates 2019 and the Establishment plan 2019.

Whereas:

(1) The final EU contribution for the European Union Agency for Network and Information Security (ENISA) in 2019 is 15.910.000,00 euros.

(2) A proposal for a Regulation of the European Parliament and of the Council, submitted by the Commission on 13 September 2017, on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) No 526/2013, and on Information and Communication Technology cybersecurity certification

[1] https://eur-lex.europa.eu/budget/data/General/2019/en/SEC03.pdf

('Cybersecurity Act') (COM(2017) 477 final) has been adopted by the European Parliament on 12 March 2019 and it is foreseen the Council of the European Union will adopt it by the end of March 2019.

(3) The Management Board shall adjust the Agency's budget and work programme in accordance with the general budget of the European Union for the financial year 2019.

HAS DECIDED TO ADOPT THE FOLLOWING DECISION:

Article 1

ENISA Programming Document 2019-2021 is amended as provided in the Annex 1.

Article 2

Following the adoption of the General budget of the European Union for the financial year 2019, ENISA budget for the financial year 2019 is adjusted as set-out in Annex 2.

Article 3

The present decision shall enter into force on the day following that of its adoption. It will be published on the Agency website.

Done by written procedure on 31.05. 2019.

On behalf of the Management Board,

[signed]

Jean-Baptiste Demaison

Chair of the Management Board of ENISA

Amendments of the Work Programme 2019, SPD 2019-2021

1 Introduction

The agreement reached in December 2018 with the Cybersecurity Act will result in a new legal basis for ENISA activities. This new legal basis is associated with additional resources and budget as outlined in the EU budget for 2019. This document details how the current version of SPD 2019 will be amended in order to take account of this new legal basis. .

The amendments are listed by section. Some amendments (*like the one addressing the cybersecurity of 5G networks*), contain changes in several sections, and are grouped together in one amendment. Each amendment is, compared against the ENISA SPD2019-2021 text approved by the ENISA Management Board in the MB decision number MB/2018/20.

2 Amendments

General amendments in view of the new Cybersecurity Act[1] and the voted 2019 budget[2].

- **Throughout the text of the SPD 2019 the words Permanent Stakeholders Group (PSG) are replaced by ENISA Advisory Group;**
- **References to Scenario 1 and Scenario 2 are removed.**

Amendment 1. Section "Foreword by the executive director", the last part is updated to reflect the changes of legal bases and the updated budget and resources.

The last part, namely section "**An agile ENISA, preparing for the future!**", the following text:

"For several years ENISA has been improving its planning and in consultation with its management board (MB) set out priorities for its activities in order to be able to deliver the most urgent, important and sensitive results for the protection our EU cyberspace. In the preparation of the 2019 work programme ENISA, together with its MB, decided to prepare the planning by considering two scenarios. These are (a) Scenario 1, which assumes no change to the current mandate and (b) Scenario 2 where it is assumed that the cybersecurity act is adopted.

In detail, Scenario 1 (assuming that the new regulation is not in place) uses the resources available in the multiannual financial framework (MFF) 2014-2020 (COM(2013)519) while Scenario 2, (new regulation in place by latest mid-2019) adds new tasks and activities as proposed in the Cybersecurity Act COM(2017)477 using resources as proposed in the draft general budget of the European Union for the financial year 2019 ().

In this programming document, the planned activities for 2019 in both scenarios are presented. The document follows the structure laid down by the new Commission guidelines for programming documents provided in the context of the framework financial regulation and the five pillars of the ENISA strategy.

---

[1] The proposed Cybersecurity Act has been politically agreed between the European Parliament, the Council and the Commission and awaits the formal approval of the co-legislature. The agreed text is available here: https://data.consilium.europa.eu/doc/document/ST-15786-2018-INIT/en/pdf

[2] General budget of the EU for the financial year 2019, Section 3 Commission, pages L67/885 for Union budget contribution and L67/1963 for authorized posts allocation under the Union budget. Available here: https://eur-lex.europa.eu/budget/data/General/2019/en/SEC03.pdf

Activities are labelled indicating to which scenario these activities belong. Activities labelled as Scenario 2 are only proposed to be delivered if the draft Cybersecurity Act is adopted. Section 'List of outputs in 2019 work programme', just before the annexes, summarises the outputs for the two scenarios: the first list covers the Scenario 1 outputs, to be delivered independent of the adoption of the cybersecurity act, while the second list includes the new outputs to be delivered as soon as the cybersecurity act is published in the Official Journal."

Is replaced by:

"**In the context of the Cybersecurity Act ([Reference 1]), 2019 marks the year that ENISA steps into a new future. ENISA is prepared and looks forward to adapting and capitalising on the opportunities of the new Regulation. The strengthened and permanent mandate and the new roles that are foreseen for ENISA lay the groundwork for an ambitious and pragmatic contribution to the cybersecurity of the EU. Encouraged by the prospect of a renewed and reinforced mandate, ENISA is ready to take on this opportunity and continue working towards a more cyber secure Union.**

This document presents the amended Work programme of the Agency for 2019, which takes account of the new budget and resources assigned to ENISA by the voted budget for 2019 [reference 2] and the Cybersecurity Act. "

With updated references:

[Reference 1] The proposed Cybersecurity Act has been politically agreed between the European Parliament, the Council and the Commission and awaits the formal approval of the co-legislature. The agreed text is available here: https://data.consilium.europa.eu/doc/document/ST-15786-2018-INIT/en/pdf

Proposal for a Regulation of the European Parliament and of the Council, submitted by the Commission on 13 September 2017, on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) No 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act') (COM(2017) 477 final).

[Reference 2] General budget of the EU for the financial year 2019, Section 3 Commission, pages L67/885 for Union budget contribution and L67/1963 for authorized posts allocation under the Union budget. Available here: https://eur-lex.europa.eu/budget/data/General/2019/en/SEC03.pdf

Amendment 2. Sections "Threat landscape" and "Policy initiatives", part of "Section I. General context" are updated.

(a) Section "Threat landscape", part of "Section I. General context", is updated based on the assessment for 2018, published in the most recent Annual Threat Analysis report

The following paragraphs:

"2017 was the year in which incidents in the cyber-threat landscape have led to the definitive recognition of some omnipresent facts. We have gained unwavering evidence on monetisation methods, attacks to democracies, cyber-war, transformation of malicious infrastructures and the dynamics within threat-agent groups.

But 2017 has also brought successful operations against cybercriminals. Law enforcement, governments and vendors have managed to shut down illegal dark markets, de-anonymise the darknet and arrest cybercriminals. Moreover, state-sponsored campaigns have been revealed and details of technologies

deployed by nation states have been leaked. Most remarkable though is the manifestation of the cyber-threat landscape within framework programmes that are about to be established in the area of critical-infrastructure protection: cyber threats make up the basis for the development and implementation of red and blue teaming activities in financial sector across Europe.

The cybersecurity community is still far from striking the balance between defenders and attackers. Although 2017 has reached records in security investment, it has also brought new records in cyberattacks of all kinds, data breaches and information loss. From this perspective, one may argue that there is a market failure in cybersecurity; that is, the increased defence levels and expenses cannot successfully reduce levels of cyber-threat exposure.

Whether this is due to a segmented cybersecurity market, lack of awareness or capabilities and skills, are topics of vivid discussions in the corresponding communities. The fact is however, that in 2017 we have seen extremely increased amounts of information on cybersecurity incidents, cyber threats and related matters deluge all kinds of media. This trend is indicative for the high level of interest assigned by the media to cybersecurity issues.

In summary, the main trends in the 2017 cyber-threat landscape were as follows.

- Complexity of attacks and sophistication of malicious actions in cyberspace continued increasing.
- Threat agent of all types have advanced in obfuscation (that is, hiding their trails).
- Malicious infrastructures continue their transformation towards multipurpose configurable functions including anonymisation, encryption, detection and evasion.
- Monetisation of cybercrime is becoming the main motive of threat agents, in particular cyber-criminals. They take advantage of the anonymity offered by digital currencies.
- State-sponsored people or organisations are one of the most omnipresent malicious agents in cyberspace. They are top concern of commercial and governmental defenders.
- Cyber-war is entering dynamically into cyberspace creating increased concerns to critical-infrastructure operators, especially in areas that experience some sort of crisis.
- Skills and capabilities are the main concerns for organisations. The extensive need for related training programmes and educational curricula remains almost unsatisfied.

All these trends are assessed and analysed by means of the content of the ENISA Threat landscape report 2017. Identified open issues leveraged on these trends and proposed policy, business and research/educational action. They serve as recommendations and are taken into account in the future activities of ENISA and its stakeholders.

In 2017 the frequency and impact of serious incidents grew. The proliferation of ransomware, for example, reached an approximate 2 000 % increase in 2017 and drew everyone's attention to the reality of cyber threats and their possible critical impacts and costs.

The cooperation between law-enforcement agencies and private-sector organisations was an important factor in identifying malicious activities and infrastructure takedowns and it is likely that such cooperation activities between communities as well as between Member States, will play an increasingly important

role both in the fight against cybercrime and in the attempt to reinforce EU systems against potential attacks.

Concluding, on top of a quite active cybercrime scene, the ENISA Threat Report has indicated that high profile (state-sponsored) attackers have advanced in line with the developments of the entire threat landscape: complexity, sophistication and advancements in capabilities have been observed for most of the threat-agent groups. While the race between the 'good' and the 'bad' guys continues, advancements in obfuscation and masquerading of threat agents make it more difficult to understand who is who. This difficulty has led to an alerting phenomenon: the user community cannot differentiate between the bad and the good and thus lose trust in commercial and even institutional players in cyberspace."

Are replaced by the paragraphs:

"**The cyberthreat landscape continues to evolve. Assessed changes are indicative for the potential of developments both at the attacker and defender sides. Those changes had as source discrete developments in motives and tactics of the most important threat agent groups, namely cyber-criminals and state-sponsored actors. Monetization motives have contributed to the appearance of crypto-miners in the top threats. State-sponsored activities have led to the assumption that there is a shift towards reducing the use of complex malicious software and infrastructures and going towards low profile social engineering attacks.**

Developments have been achieved from the side of defenders too. Through the emergence of active defence, threat agent profiling has led to a more efficient identification of attack practices and malicious artefacts, leading thus to more efficient defence techniques and attribution rates. Initial successes through the combination of cyberthreat intelligence (CTI) and traditional intelligence have been achieved. This is a clear indication about the need to open cyberthreat intelligence to other related disciplines with the aim to increase quality of assessments and attribution. Finally, defenders have increased the levels of training to compensate skill shortage in the area of cyberthreat intelligence. The vivid interest of stakeholders in such trainings is a clear indicator for their appetite in building capabilities and skills.

Recent political activities have underlined the emergence of various, quite novel developments in the perceived role of cyberspace for society and national security. Cyber-diplomacy, cyber-defence and cyber-war regulation have dominated the headlines. These developments, when transposed to actions, are expected to bring new requirements and new use cases for cyberthreat intelligence. Equally, through these developments, existing structures and processes in the area of cyberspace governance will undergo a considerable revision. These changes will affect international, European and Member States bodies. It is expected that threat actors are going to adapt their activities towards these changes, affecting thus the cyberthreat landscape in the years to come.

In summary, the main trends in cyberthreat landscape are:

- **Mail and phishing messages have become the primary malware infection vector.**
- **Exploit Kits have lost their importance in the cyberthreat landscape.**
- **Cryptominers have become an important monetization vector for cyber-criminals.**
- **State-sponsored agents increasingly target banks by using attack-vectors utilised in cyber-crime.**

- **Skill and capability building are the main focus of defenders. Public organisations struggle with staff retention due to strong competition with industry in attracting cybersecurity talents.**
- **The technical orientation of most cyberthreat intelligence produced is considered an obstacle towards awareness raising at the level of security and executive management.**
- **Cyberthreat intelligence needs to respond to increasingly automated attacks through novel approaches to utilization of automated tools and skills.**
- **The emergence of IoT environments will remain a concern due to missing protection mechanisms in low-end IoT devices and services. The need for generic IoT protection architectures/good practices will remain pressing.**
- **The absence of cyberthreat intelligence solutions for low-capability organisations/end-users needs to be addressed by vendors and governments.**

All these trends are included in the content of the ENISA Threat Landscape 2018 [new reference footnote].

"

[new reference] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

(b) Section "Policy initiatives", part of "Section I. General context", last sentence and footnote 12 is updated to reflect the change of legal basis.

The last sentence:

"ENISA welcomes the renewed cybersecurity strategy ([footnote 1]) and the proposed new cybersecurity act ([footnote 2])."

Is replaced by:

"ENISA welcomes the renewed cybersecurity strategy ([footnote 1]) and the ~~**proposed**~~ new cybersecurity act ([footnote 2])."

The footnote 2 is replaced by:

"The proposed Cybersecurity Act has been politically agreed between the European Parliament, the Council and the Commission and awaits the formal approval of the co-legislature. The agreed text is available here: https://data.consilium.europa.eu/doc/document/ST-15786-2018-INIT/en/pdf "

Amendment 3. Last 2 paragraphs of the introductory part of "Section III. Work programme 2019", are updated to reflect the change of legal basis and update of budget and resources. The change of legal basis also implies discontinuation of the so-called 'Article 14 requests'.

The last two paragraphs:

"For each activity there is an objective established that covers the actions that ENISA is carrying out in order to respond to official 'Article 14 requests', named after Article 14 of the ENISA regulation ([footnote

14]), which allows the MS and EU institutions to make direct requests to ENISA seeking assistance or advice on specific activities.

In the preparation of the 2019 work programme, ENISA is considering two scenarios. Scenario 1 uses the resources available in MFF 2014-2020 (COM(2013)519). Scenario 2 (which assumes that the new regulation will be in place by latest mid-2019), adds new tasks and activities using resources as proposed in the draft Cybersecurity Act COM(2017)477 and in alignment with the draft 2019 EU general budget. Each output is labelled accordingly as a Scenario 1 or Scenario 2 output. Activities labelled as Scenario 2 are only proposed to be delivered if the draft cybersecurity act is adopted."

Are replaced by:

"**The ENISA 2019 work programme has been amended during the first quarter of 2019 to reflect the new mandate and tasks of ENISA according to the Cybersecurity Act. The resource and budget allocations reflect the EU 2019 voted budget** [Reference 1]."

With footnote to the Budget of ENISA for 2019:

[Reference 1] General budget of the EU for the financial year 2019, Section 3 Commission, pages L67/885 for Union budget contribution and L67/1963 for authorized posts allocation under the Union budget. Available here: https://eur-lex.europa.eu/budget/data/General/2019/en/SEC03.pdf

Amendment 4. The following changes are made, to several sections, to include the new activities in the area of cybersecurity of 5G networks, to free resources for this purpose from other Outputs and to assign them to the work on 5G related activities as follows:

- **(a) Re-allocation of resources to threat analysis /assessment of the cybersecurity of 5G networks activity**
- **(b) Re-allocation of resources for the Cooperation Group activity on cybersecurity of 5G networks.**
- **(c) New text assigning coordination role on cross agency activities to Policy office, in Activity 5**

(a) Re-allocation of resources to threat analysis /assessment of the cybersecurity of 5G networks activity

To free resources required for the threat analysis /assessment of the cybersecurity of 5G networks activity, the following changes are made: the Annual threat landscape report will be delivered in Q1/2019, while the Output on restricted Info notes will be stopped at the end of Q2/2019. The FTEs freed are re-allocated to Output O.1.2.1, to the new deliverables dedicated to cybersecurity of 5G networks.

As such the Section "Output O.1.2.1 — Annual ENISA threat landscape" is extended with the next two paragraphs:

"**In the realm of its involvement in the "Cybersecurity of 5G Networks" of the Commission [**new reference**], ENISA will deliver a 5G Threat Landscape mapping. This deliverable will be based on existing ENISA work in this area (SDN/5G Threat Landscape). This work will be updated – primarily to cover the radio access part – and will serve as basis for the identification of 5G related risks and their mitigation. The ENISA 5G Threat Landscape will be created with support of relevant stakeholders, while it will be supported by the Cooperation Group and the Computer Security Incident Response Teams network.**

In support of the Member States, the Commission and relevant stakeholders, ENISA will consolidate national risk assessments performed by Member States into a single document. Together with the 5G

Threat Landscape, this Consolidated risk assessment will flow into a joint review of the Union-wide exposure to 5G networks."

A new reference is added:

[New reference] Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks C(2019) 2335 final, available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58154

Furthermore, the associated rows for the outputs O.1.2.1 and O.1.2.2 in the table "Type of outputs and performance indicators for each output of Activity 1 expertise":

Output O.1.2.1 — Annual ENISA threat landscape	P: Report and online information offering; report, Q4, information offering during the year E: ENISA will organise the annual event on CTI EU, Q3-Q4.	Engage more than 10 MS in discussions and work related to the structure and content of ENISA threat landscape report. More than 5 000 downloads of the ENISA threat landscape report. Engagement of more than 80 CTI experts from industry, academia and MSs.
Output O.1.2.2 — Restricted and public Info notes on NIS	P: Info notes on NIS, Q1-Q4.	Coverage of all major incidents relevant to EU NIS policy priorities. Expand coverage to all key ENISA stakeholder groups.

Are replaced by:

Output O.1.2.1 — Annual ENISA threat landscape	P: Report and online information offering; report, Q4, information offering during the year**, Q1/2020** E: ENISA will organise the annual event on CTI EU, Q3-Q4. **P: 5G Threat Landscape report, Q3,2019** **Consolidated risk assessment report from MS input, Q3, 2019**	Engage more than 10 MS in discussions and work related to the structure and content of ENISA threat landscape report. More than 5 000 downloads of the ENISA threat landscape report. Engagement of more than 80 CTI experts from industry, academia and MSs. **At least 7 5G Experts participate in the review of the report** **At least 18 Member States participate in the Cooperation Group team supporting the activity** **At least 10.000 views of the delivered report** **At least 10 Member States provide input to be consolidated report** **At least 5.000 views of the delivered report**
Output O.1.2.2 — Restricted and public Info notes on NIS	P: Info notes on NIS, Q1-~~Q4~~ **Q2**.	Coverage of all major incidents relevant to EU NIS policy priorities. Expand coverage to all key ENISA stakeholder groups.

(b) Re-allocation of resources for the Cooperation Group activity on cybersecurity of 5G networks.

To support cybersecurity of 5G networks related activities in the context of the Cooperation Group, to allow increasing of FTE allocation under Output O.2.2.2, some deliverables related to NISD were removed from Output O.2.2.8 and O.3.1.4.

The associated row for Output O.2.2.8 in the table "Type of outputs and performance indicators for each output of Activity 2 policy":

O.2.2.8 — Supporting the sectorial implementation of the NISD	P: NISD Sector-Specific Initiatives, Q4. S: Supporting Commission, EU agencies, MS and private sector in the sectorial implementation of two NISD sectors.	Engage 12 MS and 10 OES organisation in NISD sector-specific initiatives

Is replaced by:

O.2.2.8 — Supporting the sectorial implementation of the NISD	~~P: NISD Sector-Specific Initiatives, Q4.~~ S: Supporting Commission, EU agencies, MS and private sector in the sectorial implementation of two NISD sectors.	Engage 12 MS and 10 OES organisation in NISD sector-specific initiatives

The following paragraph in Section "Output O.3.1.4 — Support EU MS in the development of ISACs for the NISD Sectors" is removed:

"• ~~EU aviation ISAC: ENISA plays a key role in the (further) development of this ISAC. Its added value is mainly based on the network and the specific expertise in the sector (previous and existing studies). The members consist of airlines and carriers. ENISA is an associate member.~~"

The associated row for Output O.3.1.4 in the table "Type of outputs and performance indicators for each output of Activity 3 capacity":

Output O.3.1.4 — Support EU MS in the development of ISACs for the NISD Sectors	P: A toolkit for creating an EU ISAC undertaken in conjunction with CEF ISACs Facilities manager, Q4. S: Support relevant public and private stakeholders in establishing EU ISACs using the CEF funding opportunities, Q1-Q4. S: Support the Commission and facilitate alignment of the CEF EU-level sectorial ISACs Facilities Manager's tasks with work on ISACs development, Q2-Q4.	Engage at least 12 organisations representing at least 3 sectors from at least 8 MS in this activity (P).

Is replaced by:

Output O.3.1.4 — Support EU MS in the development of ISACs for the NISD Sectors	~~P: A toolkit for creating an EU ISAC undertaken in conjunction with CEF ISACs Facilities manager, Q4.~~ S: Support relevant public and private stakeholders in establishing EU ISACs using the CEF funding opportunities, Q1-Q4. S: Support the Commission and facilitate alignment of the CEF EU-level sectorial ISACs Facilities Manager's tasks with work on ISACs development, Q2-Q4.	Engage at least 12 organisations representing at least 3 sectors from at least 8 MS in this activity (~~P~~**S**).

The activities related to 5G under Output O.2.2.2 dedicated to Cooperation Group are described as following:

New paragraphs added at the end of the "Output 2.2.2 — Supporting the implementation of the work programme of the cooperation group under the NISD":

"**The Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks [new footnote for the reference] asks ENISA to support the NIS Cooperation Group and Member States with developing a so-called 5G toolbox of good practices for MS to mitigate 5G risks based on the national risk assessments and the joint risk assessment foreseen under Output 1.2.1.**

In that context, ENISA will support MS and the Commission in identifying such possible good practices mitigating the risks mentioned above and in validating them against the needs and requirements of MS. The toolbox will include appropriate security measures and recommendations to mitigate the identified cybersecurity risks both at national and Union level."

[Footnote] Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks C(2019) 2335 final, available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58154

The associated row for Output O.2.2.2 in the table "Type of outputs and performance indicators for each output of Activity 2 policy":

Output O.2.2.2 — Supporting the implementation of the work programme of the cooperation group under the NISD	S: Support the cooperation group in assessing the implementation of the NISD, Q1-Q4. S: Support the work of the cooperation group by providing in due time advice and expertise on deliverables and good practices identified by the Group in the 2018-2020 work programme, Q1-Q4. E: A workshop related to the tasks of the NISD, Q2-Q4. S: Assist cooperation group with the update of existing 'living documents' (e.g. security measures) Q1-Q4.	Engaging at least 12 MS in ENISA's contributions to the implementation of the NISD (S). 10 MS participate in the workshop/activity (E).

Is updated with one more activity and KPI, as follows:

Output O.2.2.2 — Supporting the implementation of the work programme of the cooperation group under the NISD	S: Support the cooperation group in assessing the implementation of the NISD, Q1-Q4. S: Support the work of the cooperation group by providing in due time advice and expertise on deliverables and good practices identified by the Group in the 2018-2020 work programme, Q1-Q4. E: A workshop related to the tasks of the NISD, Q2-Q4. S: Assist cooperation group with the update of existing 'living documents' (e.g. security measures) Q1-Q4. **S: Support the Cooperation Group in developing a toolbox of good practices for 5G cybersecurity. (Q4 2019)**	Engaging at least 12 MS in ENISA's contributions to the implementation of the NISD (S). 10 MS participate in the workshop/activity (E). **Engaging at least 12 MS in ENISA's contributions to Cooperation Group efforts on 5G cybersecurity (S).**

(c) New text assigning coordination role on cross agency activities to Policy office, in Activity 5

In the section "Objective 5.1. Management and compliance", the first paragraph describing Policy Unit work is updated to carry on coordination activities, for instance, for the cybersecurity of 5G networks. The paragraph:

"Policy office

Through the policy office, ENISA initiates and further develops strategic cooperation with relevant stakeholders active in cybersecurity community. For instance, ENISA engages in policy and strategy discussions with political and policy decision-makers (by participating or organising e.g. MEP breakfasts). Furthermore ENISA engages and further develops strategic relationships with e.g. specific industry sectors at decision-making level, and identifies the strategic issues on cybersecurity. Some of the results of these activities of the policy office are published as opinion papers on ENISA webpage. Besides these activities, more details of the activities delivered by policy office and Public Affairs team are detailed in Objective 5.2 Engagement with stakeholders and international activities."

Is replaced by:

"Policy office

Through the policy office, ENISA initiates and further develops strategic cooperation with relevant stakeholders active in cybersecurity community. For instance, ENISA engages in policy and strategy discussions with political and policy decision-makers (by participating or organising e.g. MEP breakfasts). Furthermore, ENISA engages and further develops strategic relationships with e.g. specific industry sectors at decision-making level, and identifies the strategic issues on cybersecurity. Some of the results of these activities of the policy office are published as opinion papers on ENISA webpage. **The policy office also coordinates cross agency activities related to topical areas of interest.** Besides these activities, more details of the activities delivered by policy office and Public Affairs team are detailed in Objective 5.2 Engagement with stakeholders and international activities."

Amendment 5. Section "Objective 1.4. Response to Article 14 requests under expertise activity" and associated outputs in the table "Type of outputs and performance indicators for each output of Activity 1 expertise" is removed to reflect the change of legal basis that implies discontinuation of the so-called 'Article 14 requests'.

The Objective 1.4 paragraphs are deleted:

"Objective 1.4. Response to Article 14 requests under expertise activity ([3])
Output O.1.4.1 — Response to requests under expertise activity (Scenario 1)
Article 14 requests allow the MS and EU institutions alike to make direct requests to ENISA when seeking assistance or advice on specific activities or policy issues. Under this objective, ENISA will address all the requests related to its area the area of expertise.

The type of outcome and the performance indicators will be set out during the execution year of the work programme together with the requester.

([3]) If Scenario 2, this objective will be reallocated based on the new framework.

Although, by definition, it is not possible to accurately estimate the exact number or the output and outcome of these requests for 2018, the allocated resources are indicated in the summary section at the end. ”

The last 2 rows in the table “Type of outputs and performance indicators for each output of Activity 1 expertise” are removed.

Objective 1.4. Response to Article 14 requests under expertise activity		
Output O.1.4.1 — Response to requests under expertise activity (Scenario 1)	S: Answers to requests.	

Amendment 6. The row for Output O.1.1.4 “Good practices for the security of healthcare services” in the table “Type of outputs and performance indicators for each output of Activity 1 expertise” is updated to reflect the merger of two complementary Support (S) activities, since their content/scope overlaps.

The table row:

Output O.1.1.4 — Good practices for the security of healthcare services (Scenario 2)	P: Procurement guidelines for cybersecurity in hospitals, Q3-Q4. S: Support the Commission and the relevant MS healthcare organisations in EU policy initiatives (e.g. JASEHN WP 2018-2020), Q1-Q4. S: Support the EU healthcare organisations in identifying risks in their systems, Q1-Q4. E: Annual eHealth workshop including validation session of the relevant studies, Q3-Q4.	Engage healthcare stakeholders from at least 12 EU MS in this activity, i.e. publication (P) and/or workshop (E) and/or support (S).

Is replaced by:

Output O.1.1.4 — Good practices for the security of healthcare services (Scenario 2)	P: Procurement guidelines for cybersecurity in hospitals, Q3-Q4. **S: Support the Commission and the relevant MS healthcare organisations in EU policy initiatives (e.g. JASEHN WP 2018-2020), Q1-Q4.** E: Annual eHealth workshop including validation session of the relevant studies, Q3-Q4.	Engage healthcare stakeholders from at least 12 EU MS in this activity, i.e. publication (P) and/or workshop (E) and/or support (S).

Amendment 7. The Output O.2.2.4 “Supporting the Payment Services Directive (PSD) implementation” is removed reflecting organisational changes while taking on board new tasks and new priorities (i.e. MeliCERTes).

The paragraphs below are removed:

“Output O.2.2.4 — Supporting the payment services directive (PSD) implementation (Scenario 1)
The second payment-services directive (PSD II) will revolutionise the finance sector and more specifically the payments industry. It will affect everything from the way payments are made online, to what information is sent when making a payment. The transposition of the directive was set as January 2018.

ENISA will continue its support for the European Banking Authority (EBA), the European Central Bank (ECB) and relevant competent public and private stakeholders to develop guidelines and recommendations for implementing the directive and explore NISD collaboration.

In this context ENISA will help the relevant authorities with presenting the security requirements and incident-reporting status for each MS on PSD II implementing the directive in with the use of a web tool.

This work item builds on previous work of ENISA in the area of supporting activities in the NISD (WP 2015-2017)."

The corresponding row for Output O.2.2.4 in the table "Type of outputs and performance indicators for each output of Activity 1 expertise" is removed:

Output O.2.2.4 — Supporting the Payment Services Directive (PSD) implementation (Scenario 1)	P: Web tool presenting the security requirements and incident-reporting status for each MS on PSD II, Q2. S: Support EBA, ECB and stakeholders of the finance sector in the implementation of the PSD2 and its synergy with the NISD. E: 2 workshops with relevant stakeholders (and EGFI, EBA) (Q2-Q4).	Engaging at least 12 Member States regulatory bodies in the workshops. Engage at least 10 financial institutions in the workshops.

Amendment 8. Section "Objective 2.3. Response to Article 14 requests under policy activity" and associated outputs in the table "Type of outputs and performance indicators for each output of Activity 2 policy" is removed to reflect the change of legal basis that implies discontinuation of the so-called 'Article 14 requests'.

The Objective 2.3 paragraphs are deleted:

"Objective 2.3. Response to Article 14 requests under policy activity ([4])

Output O.2.3.1 — Response to requests under policy activity (Scenario 1)
Article 14 requests allow the MS and EU institutions to make direct requests to ENISA seeking assistance or advice on specific activities. Under this objective, ENISA will address all the requests related to the area of policy development and policy implementation.

The type of outcome and the performance indicators will be set out during the execution year of the work programme together with the requester.

Although, by definition, it is not possible to accurately estimate the exact number or the output and outcome of these requests for 2018, the allocated resources are indicated in the summary section at the end."

The last 2 rows in the table "Type of outputs and performance indicators for each output of Activity 2 policy" are removed.

Objective 2.3. Response to Article 14 requests under policy activity		
Output O.2.3.1. Response to requests under policy activity (Scenario 1)	S: Answers to requests.	

([4]) If Scenario 2, this objective will be reallocated based on the new framework.

Amendment 9. The row for Output O.2.2.3 "Assist MS in the implementation of OES and DSPs security requirements" in the table "Type of outputs and performance indicators for each output of Activity 2 policy" is updated. Small reduction in scope by cancelling 1 out of the 2 workshops.

The table row:

Output O.2.2.3 – Assist MS in the implementation of OES and DSPs Security requirements (Scenario 1)	P: Web tool for mapping the baseline security measures to existing international standards, Q1. P: Stock Taking of security requirements set by different legal frameworks on OES and DSPs, Q4. E: Two workshops with stakeholders from OES sectors, Q2-Q4. P: Web tool for mapping the dependencies' indicators to international standards, Q3. S: Support MS in assessing the implementation of security requirements of the NISD, Q3-Q4.	Engage 12 MS in the stock taking of good practices for OES and DSPs (P). More than 10 MS and 15 OES participate in the workshops/activity (E).

Is replaced by table row:

Output O.2.2.3 – Assist MS in the implementation of OES and DSPs Security requirements (Scenario 1)	P: Web tool for mapping the baseline security measures to existing international standards, Q1. P: Stock Taking of security requirements set by different legal frameworks on OES and DSPs, Q4. E: **One** workshop with stakeholders from OES sectors, Q2-Q4. P: Web tool for mapping the dependencies' indicators to international standards, Q3. S: Support MS in assessing the implementation of security requirements of the NISD, Q3-Q4.	Engage 12 MS in the stock taking of good practices for OES and DSPs (P). More than 10 MS and 15 OES participate in the workshop/activity (E).

Amendment 10. The row for Output O.2.2.8 "Supporting the sectorial implementation of the NISD" in the table "Type of outputs and performance indicators for each output of Activity 2 policy" is updated. Small reduction in scope by cancelling two workshops and accordingly removing the corresponding KPI, because of the late start of the project it is not feasible to engage stakeholders for the organization of the workshops in time (The activity will start only after WP amendment is adopted).

The row for Output2.2.8 in the Outputs table:

O.2.2.8 — Supporting the sectorial implementation of the NISD (Scenario 2)	P: NISD Sector-Specific Initiatives, Q4. E: 2 Workshops with NISD Stakeholders, Q2, Q4. S: Supporting Commission, EU agencies, MS and private sector in the sectorial implementation of two NISD sectors.	Engage 12 MS and 10 OES organisation in NISD sector-specific initiatives Engage 12 MS and 10 OES organisation in activities/workshops.

Is replaced by row:

O.2.2.8 — Supporting the sectorial implementation of the NISD (Scenario 2)	P: NISD Sector-Specific Initiatives, Q4. ~~E: 2 Workshops with NISD Stakeholders, Q2, Q4.~~ S: Supporting Commission, EU agencies, MS and private sector in the sectorial implementation of two NISD sectors.	Engage 12 MS and 10 OES organisation in NISD sector-specific initiatives **(P) and/or (S)** ~~Engage 12 MS and 10 OES organisation in activities/workshops.~~

Amendment 11. Section "Objective 3.4. Response to Article 14 requests under capacity activity" and associated outputs in the table "Type of outputs and performance indicators for each output of Activity 3 capacity" is removed to reflect the change of legal basis that implies discontinuation of the so-called 'Article 14 requests'.

The Objective 2.3 paragraphs are deleted:

"Objective 3.4. Response to Article 14 requests under capacity activity ([5])
Output O.3.4.1 — Response to requests under capacity activity (Scenario 1)
Article 14 requests allow the MS and EU institutions to make direct requests to ENISA seeking assistance or advice on specific activities. Under this objective, ENISA will address all the requests related to the area of capacity building.

The type of outcome and the performance indicators will be set out during the execution year of the work programme together with the requester.

Although, by definition, it is not possible to accurately estimate the exact number or the output and outcome of these requests for 2018, the allocated resources are indicated in the summary section at the end."

The last 2 rows in the table "Type of outputs and performance indicators for each output of Activity 3 capacity" are removed.

Objective 3.4. Response to Article 14 requests under capacity activity		
Output O.3.4.1 — Response to requests under capacity activity (Scenario 1)	S: Answers to requests.	

Amendment 12. The row for Output O.3.1.2 "Support EU MS in the development and assessment of NCSs" in the table "Type of outputs and performance indicators for each output of Activity 3 capacity" is updated. KPI is adjusted to make it more realistic since the corresponding Support (S) action is triggered only on demand by the MS.

The row for Output 3.1.2 in the Outputs table:

Output O.3.1.2 — Support EU MS in the development and assessment of NCSS (Scenario 1)	P: Good practices in innovation on cybersecurity under the NCSS, Q3-Q4. S: Developing an information hub for NCSS in MS (Tool), Q3-Q4. S: Support MS in the deployment of an NCSS assessment methodology. E: Workshop with EU MS on NCSS development, Q2-Q4.	Engage stakeholders from at least 5 EU MS in using the NCSS assessment methodology (S) Engage stakeholders (national competent authorities or private sector) from at least 12 EU MS in this activity/workshop (P and E).

Is replaced by row:

Output O.3.1.2 — Support EU MS in the development and assessment of NCSS (Scenario 1)	P: Good practices in innovation on cybersecurity under the NCSS, Q3-Q4. S: Developing an information hub for NCSS in MS (Tool), Q3-Q4.	Engage stakeholders from at least ~~5~~**2** EU MS in using the NCSS assessment methodology (S) Engage stakeholders (national competent authorities or private sector) from at least

([5]) If Scenario 2, this objective will be reallocated based on the new framework.

	S: Support MS in the deployment of an NCSS assessment methodology. E: Workshop with EU MS on NCSS development, Q2-Q4.	12 EU MS in this activity/workshop (P and E).

Amendment 13. Update of Output O.4.1.3 with the merged activities of Outputs O.4.1.3 and O.4.1.5 into a single output. The new name is 'O.4.1.3 Supporting the implementation and further development of the cyber-crisis-collaboration blueprint '. The changes are also reflected in the table "Type of outputs and performance indicators for each output of Activity 4 community". The reason is that both outputs O.4.1.3 and O.4.1.5 concern the Blueprint development, from the perspective of the EU Institutions and from the perspective of the Member States. In order to ensure coherency in the blueprint development, these two outputs are merged into one under the description presented below.

The Outputs:

"Output O.4.1.3 — Support activities for cyber-crisis management (Scenario 1)
Since 2015, ENISA offers the secretariat to the MS developing EU-level standard cooperation procedures, which formed the basis of the CSIRTs network SOPs. ENISA will continue to support Member States in the implementation of the cyber-crisis-collaboration blueprint. In particular, ENISA will further support the maintenance of the CISRT network SOPs.

The 2016 Communication 'Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry' encouraged Member States to make the most out of the NISD cooperation mechanisms and to enhance cross-border cooperation related to preparedness for a large-scale cyber incident.

The 2017 blueprint called for the establishment of 'practical implementation guidelines as regards the integration of their national crisis management and cybersecurity entities and procedures into existing EU crises management mechanisms, namely the Integrated Political Crisis Response (IPCR) and European External Action Service Crisis Response Mechanism (EEAS CRM). In particular, Member States should ensure that appropriate structures are in place to enable the efficient flow of information between their national crisis management authorities and their representatives at EU level in the context of EU crisis mechanisms'.

In this light, ENISA will support individual Member States in setting up, improving and testing their own cyber-crisis management frameworks in order to ensure a smooth adoption of the blueprint and to foster synergies in crisis management practices across Member States. ENISA will support the cross-border cooperation between Member States, relevant authorities and facilitate the engagement with the crisis management framework at national and EU level. Activities offered will range from remote training on crisis management and public affairs handling, on-site workshops, document revision and tabletop exercises, including opportunities in CE2020 for testing national crisis management structures.

Last, building upon the after action report from Cyber Europe 2018 and in an effort to improve crisis management practices at sectorial level, ENISA will draft a report on cyber-crisis management practices in the aviation sector."

and the Output:

"Output O.4.1.5 — Supporting the implementation of the cyber-crisis-collaboration blueprint (Scenario 2)

ENISA will support EU institutions in the implementation of the cyber-crisis-collaboration blueprint. As specified in the blueprint: 'The EU cybersecurity crisis response framework should in particular identify the relevant […]EU institutions […]at all necessary levels — technical, operational, strategic/political and develop, where necessary, standard operating procedures that define the way in which these cooperate within the context of EU crisis management mechanisms. Emphasis should be placed on enabling the exchange of information without undue delay and coordinating the response during large-scale cybersecurity incidents and crises.'

In particular, ENISA will assist the Commission and the Member States in further developing bilateral and multilateral procedures for cyber-crisis cooperation with:

- DG Communications Networks, Content and Technology
- the European cybercrime centre at Europol (Europol/EC3)
- the EU intelligence and situation centre (INTCEN) at at the European External Action Service (EEAS)
- the EU military staff intelligence directorate (EUMS INT) and situation room (Sitroom) working together as the single intelligence analysis capacity (SIAC)
- the EU hybrid fusion cell (based in INTCEN)
- the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU)
- the European Commission emergency response coordination centre
- and possibly the cybersecurity emergency response fund.

ENISA will drive working groups to initiate or further develop these procedures in the context of the blueprint, from establishing emergency directories and update processes to structuring cooperation activities during crises. This is what the blueprint calls as priorities.

ENISA will assist Member States to engage EU cybersecurity crisis response framework with national cybersecurity crisis response frameworks.

Furthermore, upon request or emerging needs, ENISA will organise workshops and/or tabletop exercises to validate that these procedures allow for the exchange of information without undue delay, before their use either in real life or in larger exercises such as Cyber Europe."

Are replaced by the Output:

"Output O.4.1.3 — Supporting the implementation and further development of the cyber-crisis-collaboration blueprint

ENISA will support the implementation and further development of the cyber crisis collaboration blueprint. As specified in the blueprint: 'Cyber crisis response activities should be coordinated with other crisis management mechanisms at EU, national or sectoral levels. '

In particular, ENISA will support:

a. the Commission in further developing bilateral and multilateral Standard Operating Procedures (SOPs) for cyber-crisis cooperation with EU bodies and Institutions:

b. Member States, either through the NIS Cooperation Group activities or after individual requests by Member States for support in the development of Blueprint SOPs at a National level.

In addition, ENISA will support EU Institutions and Member States in testing their crisis management structures. Activities offered will range from remote training on crisis management and public affairs

handling, on-site workshops, document revision and table-top exercises, including opportunities in CE2020 for testing national crisis management structures."

The rows corresponding to Outputs O.4.1.3 and O.4.1.5 in the table "Type of outputs and performance indicators for each output of Activity 4 community" are changed from:

Output O.4.1.3 — Support activities for cyber-crisis management (Scenario 1)	P: Report on good practices in cyber-crisis cooperation and management in aviation, Q4.	At least 5 stakeholders of the Aviation sector from EU MS consulted.
Output O.4.1.5 — Supporting the implementation of the cyber-crisis-collaboration blueprint (Scenario 2)	P: Q4 Supporting the implementation of the cyber-crisis collaboration blueprint.	At least 5 stakeholders from EU MS consulted.

As shown below:

Output O.4.1.3 — Supporting **the implementation of the cyber-crisis-collaboration blueprint** (Scenario 1)	**P: Identify missing elements in the Cybersecurity Blueprint and exercise the CSIRTs network SOPs.**	**At least 2 exercises on the Blueprint collaboration.**
~~Output O.4.1.5 — Supporting the implementation of the cyber-crisis-collaboration blueprint (Scenario 2)~~	~~P: Q4 Supporting the implementation of the cyber-crisis collaboration blueprint.~~	~~At least 5 stakeholders from EU MS consulted.~~

Amendment 14.' Output O.4.1.4 Supporting the implementation of the information hub' is modified. The two last paragraphs in the output description are amended to reflect latest developments for the information hub (OpenCSAM). The row for Output O.4.1.4 in the table "Type of outputs and performance indicators for each output of Activity 4 community" is also updated.

The two last paragraphs:

"In order to support the drafting of these reports and process meaningfully the massive inputs they require, ENISA has developed in 2018 a prototype to perform automatic classification of documents as well as simple automatic generation of reports by applying Natural Language Processing and Machine Learning techniques. This prototype is the first brick of a toolset meant to assist in the development of EU cybersecurity situation reports, supporting a steady increase and offering guarantees in production time, quality and consistency.

For this particular output, ENISA will leverage the experience gained in drafting EU Cybersecurity Technical Situation Reports with the prototype to further develop the Natural Language Processing features in order for the tool to transition from paragraph-based proposals to the production of meaningful sentences. Similarly, this experience will be leveraged to further develop the Machine Learning algorithms of the prototype to allow for a significant increase in number and type of information sources."

Are replaced by paragraphs:

''In order to better support the fusion of Open Source information for these reports, ENISA has developed in 2018 a prototype called 'Open Cyber Situational Awareness Machine (OpenCSAM)' to perform open source information aggregation, automatic classification of documents as well as simple automatic generation of reports by applying Natural Language Processing and Machine Learning techniques. This prototype is the first brick of a capability meant to assist in the development of EU

cybersecurity situation reports, supporting a steady increase and offering guarantees in production time, quality and consistency.

For this particular output, ENISA will leverage the experience gained from the first prototype in order to further develop OpenCSAM's functionalities and capabilities. ENISA will also foster the development of a community (Member States, Academia, Private Sector, EU Institutions) around OpenCSAM for getting contributions, feedback and evaluation during the development lifecycle. For this, a workshop is planned to take place in 2019 as well as a testing phase for the new functionalities OpenCSAM with an EU Institution related to the Aviation/Space sector.'

The row for Output O.4.1.4 in the Outputs tables:

Output O.4.1.4 — Supporting the implementation of the information hub (Scenario 2)	S: Support for other EU agencies having a role in cybersecurity.	Established communication procedures with all affected agencies and EU bodies having a role in cybersecurity.

Is replaced by:

Output O.4.1.4 — Supporting the implementation of the information hub (Scenario 2)	S: ~~Support for other EU agencies having a role in cybersecurity.~~ **Enhance Blueprint stakeholders' situational awareness.**	~~Established communication procedures with all affected agencies and EU bodies having a role in cybersecurity.~~ **Provision of OpenCSAM tool to Blueprint stakeholders in Cyber Europe 2020.**

Amendment 15. Output O.4.2.3 — Supporting the implementation and development of the MeliCERTes platform (Scenario 1) in split into two parts. Under O.4.2.3 the operational support for MeliCERTes is maintained while the systems related tasks are moved under IT in Activity 5, Objective 5.1. As such,

(a) the Output 4.2.3 is re-written,
(b) the associated activities and KPIs are updated in the table "Type of outputs and performance indicators for each output of Activity 4 community" and
(c) a new paragraph is added in section IT under Activity 5, Objective 5.1 to cover MeliCERTes systems. Some additional budget freed from Title 3 was also re-allocated to this activity in Title 2.

The paragraphs of Output O.4.2.3:

"By the end of 2019, ENISA will take over the central component of MeliCERTes, which is destined to be the primary collaboration platform between participating Member States CSIRTs and which is oriented to enlarge EU MS preparedness, cooperation and coordination to effectively respond to emerging cyber threats as well as to cross-border incidents. ENISA will also work together with the Commission to set out (a) the extent of support for the implementation of MeliCERTes running in the CSIRTs premises and (b) the support for the maintenance of the underlying codebase of the MeliCERTes system. Based on this work, we will establish corresponding procedures and service level agreement (SLAs) for the support and work with the Commission to ensure that the code base is correctly supported. In particular ENISA with the endorsement of the Commission will lead on the development and finalisation of a sustainable governance arrangement for MeliCERTes with the enabling legal requirements for the participating Member States. ENISA also will support the work of the Commission in resourcing capabilities on cybersecurity through CEF calls under the objectives of the NISD, including assistance in the preparatory phase of CEF proposals related with the support of MeliCERTes platform.

Due to the sensitivity of the data and the level of trust required by our stakeholders, special care and diligence is needed in order to correctly plan, deploy, administrate and maintain the different systems

related with MeliCERTes platform, therefore high standards of security must be reached in order to provide internal and external secure operation capabilities, continuous integration of the software and support to users.

During 2019, ENISA will deploy different systems and processes with the aim of being able to support, maintain and develop the platform and related activities, including collaboration, involvement and alignment on cyber exercises and on the CSIRTs network."

Are all replaced by the new paragraphs for O.4.2.3:

"**By the end of 2019, ENISA will take over the central component of MeliCERTes, which is destined to be the primary collaboration platform between participating Member States CSIRTs and which is oriented to enlarge EU MS preparedness, cooperation and coordination to effectively respond to emerging cyber threats as well as to cross-border incidents.**

In 2019, ENISA will actively support the platform handover procedure from an operational perspective (Trust Circles management). In particular, ENISA will engage in cooperation with the Commission and the Consortium for a smooth transition of the knowledge and expertise regarding the Trust Circles management task. Additionally, specific operational procedures that are mandatory to follow in order to maintain the underlying team data and references will be implemented by ENISA."

The row for Output 4.2.3 in the Output table:

Output O.4.2.3 — Supporting the implementation and development of MeliCERTes platform (Scenario 1)	P: Q4 Takeover of the central component of MeliCERTes: Project management support and technical assistance to the Commission, encompassing assistance with procurement as appropriate in respect of the acquisition of MeliCERTes. P: Q4 Agree responsibilities of ENISA for (a) level of support for remote components of the system and (b) management of the code base.	Engage the Member State authorities on strategy and resourcing and also the CSIRTs network members for technical and operational support.

Is replaced by:

Output O.4.2.3 — Supporting the implementation of MeliCERTes platform (Scenario 1)	~~P: Q4 Takeover of the central component of MeliCERTes: Project management support and technical assistance to the Commission, encompassing assistance with procurement as appropriate in respect of the acquisition of MeliCERTes.~~ ~~P: Q4 Agree responsibilities of ENISA for (a) level of support for remote components of the system and (b) management of the code base.~~ **S: Operational support for the MeliCERTes platform handover procedure specifically for 'Trust Circles management' task.**	~~Engage the Member State authorities on strategy and resourcing and also the CSIRTs network members for technical and operational support.~~ **Engage in cooperation with the Commission and the Consortium for a smooth transition of the knowledge and expertise regarding the Trust Circles management task and related services.**

At the end of the section "IT", in Activity 5, Objective 5.1 some new paragraphs dedicated to MeliCERTes are added:

"MeliCERTes. Depending on the agreements with the European Commission, it is foreseen that as of November 2019, ENISA will take over the central component of MeliCERTes. It is envisaged that MeliCERTes will be the primary collaboration platform between participating Member States CSIRTs as well

as to improve EU MS preparedness, cooperation and coordination, in order to better responding to emerging cyber threats as well as to cross-border incidents.

Negotiations are still undergoing with the European Commission to define the full scope of the components of the project to be taken over by ENISA, such as software development, helpdesk, etc.

The Corporate Services unit within the ENISA Resources Department will recruit two experts, which will be responsible for the project transition, in close collaboration with the European Commission and Consortium of providers. They will also be in charge of procuring equipment, setting up infrastructure and running/maintaining the infrastructure and other tasks as defined."

Amendment 16. Section "Objective 4.3. Response to Article 14 requests under community activity" and associated outputs in the table "Type of outputs and performance indicators for each output of Activity 4 community" is removed to reflect the change of legal basis that implies discontinuation of the so-called 'Article 14 requests'.

The Objective 4.3 paragraphs are deleted:

"Objective 4.3. Response to Article 14 Requests under community activity ([6])

Output O.4.3.1 — Response to requests under community-building activity (Scenario 1)
Article 14 requests allow the MS and EU institutions to make direct requests to ENISA seeking assistance or advice on specific activities. Under this objective, ENISA will address all the requests related to the area of community building, exercises and CSIRTs cooperation.

The type of outcome and the performance indicators will be set out during the execution year of the work programme together with the requester.

Although, by definition, it is not possible to accurately estimate the exact number or the output and outcome of these requests for 2018, the allocated resources are indicated in the summary section at the end. "

The rows associated for article 14 requests in the Outputs table are removed:

Objective 4.3. Response to Article 14 requests under community activity		
Output O.4.3.1 — Response to requests under community activity (Scenario 1)	S: Answers to requests.	

Amendment 17. Sections in Objective 5.1 Management and Compliance and in Objective 5.2 are updated to reflect the new legal basis. Changes include removing reference to Scenario 2, while updating information reflecting CSA:

- **(a) For MB there will be 2 meetings organized and some editorial changes introduced for resource department**
- **(b) Edits under Policy Office, Internal control , IT sections as well as in the title of Finance and procurement section**
- **(c) The permanent stakeholders group (PSG) changes name to ENISA Advisory Group.**

([6]) If Scenario 2, this objective will be reallocated based on the new framework.

- **(d) The section dedicated to PSG has been revised.**
- **(e) NLO activities are now supported by the new legal basis.**
- **(f) The section on International relations updated to reflect the new legal basis.**

(a) The paragraphs under Objective 5.1, subsection Management:

"In relation to the MB, following the applicable rules, one or two (Scenario 2) ordinary meetings will be organised during 2019 and informal meetings will be held as necessary. The MB portal will be supported for EB and MB. In relation to the executive board, one formal meeting will be organised per quarter and informal meetings when necessary.

The **resources department** (RD) oversees a variety of programmes, projects and services on the overall management of ENISA, supporting the executive director Decision is areas as personnel, finance, communications, press, purchasing, technology, facilities management, health, safety, security, protocol, liaison with local authorities, etc."

Are replaced by:

"In relation to the MB, following the applicable rules, ~~one or~~ two ~~(Scenario 2)~~ ordinary meetings will be organised during 2019 and informal meetings will be held as necessary. The MB portal will be supported for EB and MB. In relation to the executive board, one formal meeting will be organised per quarter and informal meetings when necessary.

The **resources department** (RD) oversees a variety of programmes, projects and services on the overall management of ENISA, **assisting** ~~supporting~~ the executive director ~~Decision is~~ **in** areas as personnel, finance, communications, press, purchasing, technology, facilities management, health, safety, security, protocol, liaison with local authorities, etc."

(b) Edits under Policy Office, Internal control and IT sections as well as updating the title of Finance, accounting and procurement section.

The paragraph under Policy office:

"Quality management is part of the policy office. ENISA implements a quality management system (QMS) to support its regulatory and strategic goals by means of a quality management approach. The methodology is based on the plan-do-check-act (PDCA) cycle, documented in a dedicated SOPs and applied accordingly. Planning activities of ENISA, including single programming document preparation and work programme coordination are part of policy office list of tasks. "

Is replaced by:

"Quality management is **a key corporate tool** ~~part of the policy office. ENISA implements a quality management system (QMS) to~~ support**ing** ~~its~~ regulatory and strategic goals by means of a quality management approach. The methodology is based on the plan-do-check-act (PDCA) cycle, documented in a dedicated SOPs and applied accordingly. Planning activities of ENISA, including single programming document preparation and work programme coordination are part of policy office list of tasks."

The paragraph under Internal control section:

"ENISA is aiming implement the new Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework 2013 as well as its new requirements in order to be align with the European Commission."

Is replaced by"

"**Head of Resources Department is delegated to be the Internal Control Coordinator of** ENISA. **It** is aiming **to** implement the new Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework 2013 as well as its new requirements in order to be align with the European Commission."

The paragraphs under the IT section:

"ENISA has launched a project that will run during the second half of 2018 in order to assess information-security risks and determine missing or out of date IT operational procedures. The project will provide a roadmap and the changes needed in order to mitigate the identified risks. IT Advisory Committee has decided that data the development of a datacentre recovery site is absolutely necessary in order to enhance the IT service availability.

By end of 2019 it is expected that all business applications will be securely available on the most widely used mobile devices. By this timeframe the platform consolidation should be complete and mature, with adequate, flexible and advance reporting and monitoring tools. Is expected that 2018 will consolidate the support technology in ENISA with modern, adequate and flexible business applications.

IT is supporting the implementation of a Stakeholders Relationship Management application that will support the overall stakeholder's management, communications and internal information sharing. This application also involves an effective event management platform and internal case management to be used as service internal client support for requests."

Are replaced by:

"ENISA has launched a project that will run during the second half of 201~~8~~**9** in order to assess **and improve** information-security risks and determine missing or out of date IT operational procedures. The project will provide a roadmap and the changes needed in order to mitigate the identified risks. IT Advisory Committee has decided that ~~data~~ the development of a datacentre recovery site is absolutely necessary in order to enhance the IT service availability **planned to be implemented in 2019**.

By end of 2019 it is expected that all business applications**, depending on the risk assessment,** will be securely available on the most widely used mobile devices. By this timeframe the platform consolidation should be complete and mature, with adequate, flexible and advance reporting and monitoring tools. Is expected that **in** 201~~8~~**9** ~~will~~ **to** consolidate the support technology in ENISA with modern, adequate and flexible business applications.

~~IT is supporting the implementation of a~~ **The** Stakeholders Relationship Management application **has been delivered and is available for** ~~that will support the~~ overall stakeholder's management, communications and internal information sharing. This application also involves an effective event management platform and internal case management to be used as service internal client support for requests."

"Finance, accounting and procurement" section title is changed to "Finance~~, accounting~~ and procurement".

(c) In the paragraph under Objective 5.1, subsection Management, The permanent stakeholders group (PSG) changes name to ENISA Advisory Group:

"The core operations department (COD) coordinates the delivery of the core activities of ENISA. As such, the main role of the COD is to deliver activities A1-A4 of this work programme. The COD also includes the policy office and the public affairs team and the support of ~~the permanent Stakeholders group (PSG)~~ **the ENISA Advisory Group** and national liaison officers (NLO) network is also carried out within COD."

(d) The section dedicated to PSG is revised to cover the tasks of ENISA Advisory Group. As such the section:

"Permanent stakeholders group

In 2019, ENISA will continue to support the PSG and will aim to reinforce the contribution of the PSG to the ENISA work programme.

The PSG is composed of 'nominated members' and members appointed 'ad personam'. The total number of members is 33 and they come from all over Europe. These members constitute a multidisciplinary group deriving from industry, academia and consumer organisations and are selected upon the basis of their own specific expertise and personal merits. Three (3) 'nominated members' represent national regulatory authorities, data protection and law-enforcement authorities.

The PSG is established by the ENISA Regulation (EU) No 526/2013. The MB, acting on a proposal by the executive director, sets up a PSG for a term of office of 2.5 years.

A new PSG was elected in 2017.The Role of the PSG group is to advise the executive director on the development of ENISA's work programme, and on ensuring the communication with the relevant stakeholders on all related issues."

Changes to:

"~~Permanent stakeholders group~~ ENISA Advisory Group

In 2019, ENISA will continue to support the **ENISA Advisory Group** ~~PSG~~ and will aim to reinforce the contribution of **this group** ~~the PSG~~ to the ENISA work programme.

~~The PSG is composed of 'nominated members' and members appointed 'ad personam'. The total number of members is 33 and they come from all over Europe. These members constitute a multidisciplinary group deriving from industry, academia and consumer organisations and are selected upon the basis of their own specific expertise and personal merits. Three (3) 'nominated members' represent national regulatory authorities, data protection and law-enforcement authorities.~~

The ~~PSG~~ **ENISA Advisory Group** is established by the ~~ENISA Regulation (EU) No 526/2013~~ **Cybersecurity Act**. ~~The MB, acting on a proposal by the executive director, sets up a PSG for a term of office of 2.5 years.~~ **It is envisaged that two meetings of the ENISA Advisory Group will take place during 2019.**

~~A new PSG was elected in 2017.The Role of the PSG group is to advise the executive director on the development of ENISA's work programme, and on ensuring the communication with the relevant stakeholders on all related issues.~~"

(e) NLO activities are now supported by the new legal basis and the corresponding section is updated.

The section on NLO:

"National liaison officer network

ENISA in 2017 has kicked off various activities aiming at strengthening the cooperation with its NLO network. These activities were continued and were further prepared in 2018. NLOs are key actors for ENISA's daily work and they warrant the interaction with select public sector entities in the MS while they provide assurance in outreach, effective liaison with the MS and dissemination of ENISA deliverables.

ENISA will build upon these activities and strength its cooperation with the NLO network, as the first point of contact for ENISA in the MS, with emphasis on:

- NLO meetings to discuss possible improvements in the collaboration with ENISA and input on selected ENISA projects. Improvements aim at leveraging on the NLO network for the dissemination of ENISA's work to the EU Member States and EFTA countries.
- The members of the NLO network will continue to receive information on ENISA deliverables, upcoming ENISA project related tenders, news, working groups entailing requests for identification of experts in the MS, vacancy notices, and events organised by ENISA or where ENISA contributes to (for example co-organiser, etc.) as well as time-critical information.
- ENISA maintaining and sharing with the NLO network information on all relevant ENISA projects and activities (e.g. unit responsible for the project, relevant tender results, etc.) while maintaining and expanding as appropriate online resources available.

Additionally, guidelines provided by the MB on missions, objectives and functioning of the NLO network will guide the development of this important tool for ENISA for community building."

Is replaced by the new section:

"National liaison officer network

ENISA in 2017 has kicked off various activities aiming at strengthening the cooperation with its NLO network. These activities were continued and were further prepared in 2018. NLOs are key actors for ENISA's daily work and they warrant the interaction with select public sector entities in the MS while they provide assurance in outreach, effective liaison with the MS and dissemination of ENISA deliverables.

ENISA will build upon these activities and strength its cooperation with the NLO network, as the first point of contact for ENISA in the MS, with emphasis on:

- NLO meetings to discuss possible improvements in the collaboration with ENISA and input on selected ENISA projects. Improvements aim at leveraging on the NLO network for the dissemination of ENISA's work to the EU Member States and EFTA countries.
- The members of the NLO network will continue to receive information on ENISA deliverables, upcoming ENISA project related tenders, news, working groups entailing requests for identification of experts in the MS, vacancy notices, and events organised by ENISA or where ENISA contributes to (for example co-organiser, etc.) as well as time-critical information.
- ENISA maintaining and sharing with the NLO network information on all relevant ENISA projects and activities (e.g. unit responsible for the project, relevant tender results, etc.) while maintaining and expanding as appropriate online resources available.

Additionally, guidelines provided by the MB on missions, objectives and functioning of the NLO network will guide the development of this important tool for ENISA for community building. **It is envisaged that two meetings of the NLO network will take place during 2019.** ”

(f) The paragraphs on International relations is revised to be aligned to the new Cybersecurity Act.

The section:

“International relations
Under the executive director’s guidance and initiative, ENISA will seek to strengthen contacts at an international level.

ENISA should participate in international cybersecurity fora such as the OECD, ICANN, IGF in so far as these groups are discussing items related to our work programme or strategy.

- Acting within its mandate, ENISA will develop contacts with important cybersecurity bodies outside the EU where synergies are beneficial to the EU cybersecurity programme. An example is NIST, which plays an important role in the implementation of the US Executive Order.
- Starting 2018 ENISA will follow standards development and certification initiatives at the international level, as some of the issues to be solved in the EU have international scope (notably common criteria certification).
- ENISA will follow the development of relevant subjects at the international level in order to align EU activities with other global players. An example here is provided by the work that ITU is doing with CSIRTs, which needs to be aligned and will create added value and harmonisation to all.
- ENISA staff will attend international conferences on an ‘as needed’ basis. For instance, the Meridian Conference is the main CIIP conference of the year and the FIRST conference plays the same role for CERTs.
- The ED should attend international conferences in order to enhance ENISA visibility.”

Is replaced by the section:

“International relations
Under the executive director’s guidance and initiative, ENISA will seek to strengthen contacts at an international level **in line with the relevant provisions of the new Cybersecurity Act.**

~~ENISA should participate in international cybersecurity fora such as the OECD, ICANN, IGF in so far as these groups are discussing items related to our work programme or strategy.~~

- ~~Acting within its mandate, ENISA will develop contacts with important cybersecurity bodies outside the EU where synergies are beneficial to the EU cybersecurity programme. An example is NIST, which plays an important role in the implementation of the US Executive Order.~~
- ~~Starting 2018 ENISA will follow standards development and certification initiatives at the international level, as some of the issues to be solved in the EU have international scope (notably common criteria certification).~~
- ~~ENISA will follow the development of relevant subjects at the international level in order to align EU activities with other global players. An example here is provided by the work that ITU is doing with CSIRTs, which needs to be aligned and will create added value and harmonisation to all.~~

- ~~ENISA staff will attend international conferences on an 'as needed' basis. For instance, the Meridian Conference is the main CIIP conference of the year and the FIRST conference plays the same role for CERTs.~~
- ~~The ED should attend international conferences in order to enhance ENISA visibility~~."

Amendment 18. Section "Dissemination and Outreach" is slightly modified to reflect organisational changes.

The first two paragraphs in the section:

"Dissemination and Outreach

ENISA will continue developing various tools and channels including the website and with strong emphases in social media. Dissemination activities are the responsibility of the Stakeholders Communication team that will seek the appropriate level of outreach activities to take ENISA´s work to all interested and to provide added value to Europe.

ENISA´s image of quality and trust is paramount for all stakeholders. It is indubitable the importance that all areas of our society trust in ENISA´s work. The cybersecurity challenges are increasing in the world and Europe is not an exception. With this objective ENISA´s image needs to be continuously reinforced. The outreach of ENISA work is essential to create the NIS culture across the several actors in Europe. ENISA is consistent of this fact and will work with all interested to reach the people that require information about the work that is developed by ENISA."

are replaced by:

"Dissemination and Outreach

ENISA will continue developing various tools and channels including the website and with strong emphases in social media. ~~Dissemination activities are the responsibility of the Stakeholders Communication team that will seek the appropriate level of outreach activities to take ENISA´s work to all interested and to provide added value to Europe.~~

~~ENISA´s image of quality and trust is paramount for all stakeholders. It is indubitable the importance that all areas of our society trust in ENISA´s work. The cybersecurity challenges are increasing in the world and Europe is not an exception. With this objective ENISA´s image needs to be continuously reinforced. The outreach of ENISA work is essential to create the NIS culture across the several actors in Europe. ENISA is consistent of this fact and will work with all interested to reach the people that require information about the work that is developed by ENISA.~~"

Amendment 19. Section Human Resources under Objective 5.1. Management and Compliance and section Internal communication under Objective 5.2. Engagement with stakeholders and international activities Stakeholders communication and dissemination activities are adjusted to reflect the updated functions in the agency. The whole paragraph of internal communications has been revised due to the fact that the function is now under HR. In addition, the associated KPI was moved from HR section to Internal communication section.

The first paragraph in the section internal communication under Objective 5.2:

"Stakeholders' communications comprise the internal and external stakeholders. From an internal perspective the team is responsible to support the internal communication activities aim to keep all those working within ENISA informed and to enable both management and staff to fulfil their responsibilities effectively and efficiently. A strong corporate culture improves staff engagement and ultimately the

implementation of the work programme. ENISA plans to undertake an annual review of this strategy to ensure that it is kept up to date and appropriate."

Is replaced by the new text:

"**In 2019, ENISA will strengthen internal communications to enhance staff engagement and to exploit opportunities for pooling and sharing. With the internal communication function being now under the HR unit, the objectives are:**

- **To enhance the accessibility of key HR information for staff members and managers**
- **To establish an internal communications strategy which is consistent and reflect the Agency's strategic vision**
- **To develop internal communication processes/tools/channels/guidance document to support any organisational change**
- **To ensure staff is engaged (e.g.: launching of regular staff survey, dedicated staff survey, etc)**
- **To support the evolution/change of ENISA corporate culture**."

The indicator below has been moved from HR section (Objective 5.1) to Internal communications section (Objective 5.2):

Staff Survey	**Participation of staff in the staff survey**	**65 %**	**70 %**	**75 %**

Amendment 20. Section 'List of Outputs: work programme 2019' is updated based on above listed amendments. The introductory text explain the two scenarios is removed.

The new list of outputs, **after amendment**, is:

Activity 1 - Expertise. Anticipate and support Europe in facing emerging network and information-security challenges
Objective 1.1. Improving the expertise related to network and information security (NIS)
Output O.1.1.1 - Good practices for the security of the internet of things (IoT)
Output O.1.1.2 - Good practices for the security of smart cars
Output O.1.1.3 - Awareness raising on existing technical specifications for cryptographic algorithms
Output O.1.1.4 - Good practices for the security of healthcare services
Output O.1.1.5 - Good practices for maritime security (port security)
Objective 1.2. NIS threat landscape and analysis
Output O.1.2.1 - Annual ENISA threat landscape
Output O.1.2.2 - Restricted and public Info notes on NIS
Output O.1.2.3 - Support incident-reporting activities in the EU
Output O.1.2.4 - Regular technical reports on cybersecurity situation
Objective 1.3. Research, development and innovation (RDI)
Output O.1.3.1 - Supporting cPPP in establishing priorities for EU research & development
Activity 2 - Policy. Promote network and information security as an EU policy priority
Objective 2.1. Supporting EU policy development
Output O.2.1.1 - Support the preparatory policy discussions in the area of certification of products and services
Objective 2.2. Supporting EU policy implementation
Output O.2.2.1 - Recommendations supporting implementation of the eIDAS regulation
Output O.2.2.2 - Supporting the implementation of the work programme of the cooperation group under the NISD
Output O.2.2.3 - Assist MS in the implementation of OES and DSP security requirements
Output O.2.2.4 - [Output removed following the amendment of WP19.]

Output O.2.2.5 - Contribute to the EU policy in the area of privacy and data protection with policy input on security measures
Output O.2.2.6 - Guidelines for the European standardisation in ICT security
Output O.2.2.7 - Supporting the implementation of European Electronic Communications Code (EECC)
Output O.2.2.8- Supporting the sectorial implementation of the NISD
Output O.2.2.9 - Hands on tasks in the area of certification of products and services
Activity 3 - Capacity. Support Europe maintaining state-of-the-art network and information-security capacities
Objective 3.1. Assist Member State capacity building
Output O.3.1.1 - Update and provide technical training for MS and EU bodies
Output O.3.1.2 - Support EU MS in the development and assessment of NCSs
Output O.3.1.3 - Support EU MS in their incident-response development
Output O.3.1.4 - Support EU MS in the development of ISACs for the NISD Sectors
Objective 3.2. Support EU institutions' capacity building.
Output O.3.2.1. Representation of ENISA on the Steering Board of CERT-EU and coordination with other EU agencies using the CERT-EU service
Output O.3.2.2. Cooperation with relevant EU bodies on initiatives covering NIS dimension related to their missions
Objective 3.3. Assist in improving private sector capacity building and general awareness
Output O.3.3.1 - European cybersecurity challenges (ECSC)
Output O.3.3.2 - European cybersecurity month (ECSM) deployment
Output O.3.3.3 - Support EU MS in cybersecurity skills development
Activity 4 - Community. Foster the emerging European network and information-security community
Objective 4.1. Cyber-crisis cooperation
Output O.4.1.1 - Planning of cyber Europe 2020 and cyber SOPEx
Output O.4.1.2 - Support activities for cyber exercises
Output O.4.1.3 - Support the implementation and further development of the cyber-crisis-collaboration blueprint
Output O.4.1.4 - Supporting the implementation of the information hub
Output O.4.1.5 - [Output removed following the amendment of WP19.]
Objective 4.2. CSIRT and other NIS community building
Output O.4.2.1 - EU CSIRTs network secretariat and support for EU CSIRTs network community building
Output O.4.2.2 - Support the fight against cybercrime and collaboration between CSIRTs and law enforcement
Output O.4.2.3 - Supporting the implementation and development of MeliCERTes platform

Amendment 21 of ANNEXES A. Annexes A are updated to reflect the changes of legal bases and the updated budget and resources. In addition, the organisational chart is updated and it reflects organisational changes (i.e. taking on board new tasks and new priorities like MeliCERTes or the cybersecurity of 5G networks). The changes are covering:

- **(a) Annex A.I. Resource allocation, the text is updated as well as the tables and the charts;**
- **(b) Annex II. The following tables are updated: Table 1 Expenditure overview, Commitment appropriations and Payments appropriations, Table 2. Revenue overview and Commitment appropriations and Payments appropriations as well as Table 3 — Budget out-turn and cancellation of appropriations. Calculation of budget out-turn are replaced. The new values are based on the voted 2019 budget.**
- **(c) Annex III Human resources – Quantitative has minimum changes, as the previous numbers detailed in 'Scenario 2' match the voted resources. As such in the 'Table 1 — Staff population and its evolution; overview of all categories of staff' and in table 'Table 2 — Multiannual staff policy plan 2019-2021' column for Scenario 1 is removed as well as the reference to 'Scenario 2' in the column for 2019 staff population.**
- **(d) Annex IV: Human resources — Qualitative, sections 'A. Recruitment policy', and 'C. Mobility policy' have minor updates.**
- **(e) Annex IX: Procurement plan 2019 is updated to reflect the new voted budget.**
- **(f) Annex X: ENISA organisation is updated with a new organisation chart.**

(a) Annex A.I. Resource allocation, text updated as well as tables and charts;

In the sub-section 'Overview of the past and current situation', two paragraphs referring to the scenarios are removed and the remaining text is:

"WP 2019 is following the COM guidelines and MB decisions. The work programme is structured following the objectives and the priorities of ENISA as described in the ENISA strategy.

ENISA's budget: the variations between the years 2017 and 2018 is neutral. The budget remained with the same amount aligned with COM communications.

In 2018 a slight increase in the title II was adopted. In 2019, the budget of Title III was optimised in order to increase the budget in operations.

~~As already presented, in the preparation of work programme 2019, ENISA is considering two scenarios. In detail, Scenario 1, uses the resources available in MFF 2014-2020 (COM(2013)519). Scenario 2, (which assumes new regulation in place by latest mid-2019), adds new tasks and activities as proposed in the Cybersecurity Act COM(2017)477, using resources planned in the draft general budget of the European Union for the financial year 2019 ( ).~~

~~In case of adoption of the European Commission's proposal for ENISA's new mandate COM(2017) 477 Final, all Titles will be increased in order to deliver the proposals of the new mandate.~~

The human and financial resources of past and current situation are presented in the Annexes of this document."

In sub-section 'Resource programming for the years 2019-2021' some paragraphs are removed or updated.

The paragraphs below are removed.

"~~Following the publication of the NIS Directive (NISD), ENISA is re-allocating budget and resources to the new tasks/activities provisioned for ENISA in the directive. Another area which will probably require more budget /resources is the cybersecurity public-private partnership (cPPP). However, the impact on the ENISA work programme has not yet been quantified. This will be updated in future versions as any other relevant change in the ENISA scope and tasks~~."

"~~In addition, this version of the work programme takes account of the prioritisation exercise carried out during the consultation with the MB. Certain activities had to be removed from the work programme as there are not enough resources for the year 2018. Such de-prioritise activities are the following.~~

- ~~Activities to support a digital single market for high-quality NIS products and services.~~
- ~~Support the assessment of existing policies/procedures/practices on NIS within EU institutions.~~
- ~~Planning and organisation of EuroSOPEx 2018~~."

New footnote was added to clarify that 2018 values in the Job type table will be updated in the next version of 2020 Single Programming Document:

[footnote] "2018 values are part of the final Single Programming Document 2020-2022."

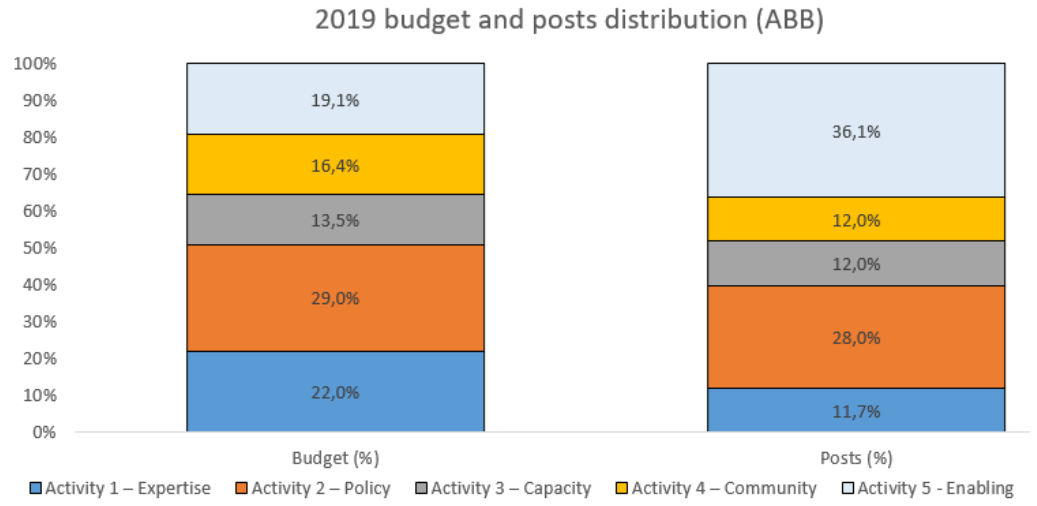
The last paragraph in sub-section 'Resource programming for the years 2019-2021', is changed and the footnote updated to reflect the 2019 voted budget for the Agency:

"The budget and resources allocations within the summary tables and Annexes ~~in Scenario 1 are in line with COM(2013)519. The budget and resources allocations within the summary tables and Annexes in Scenario 2~~ are in line with the ~~proposed~~ additional resources and budget in the ~~draft~~ **voted** general budget of the European Union for the financial year 2019 ([new footnote])."

The new footnote is:

"General budget of the EU for the financial year 2019, Section 3 Commission, pages L67/885 for Union budget contribution and L67/1963 for authorized posts allocation under the Union budget. Available here: https://eur-lex.europa.eu/budget/data/General/2019/en/SEC03.pdf "

The updated chart is as follows:



The last paragraph in sub-section 'Overview of activities budget and resources', is changed to remove references to scenarios and the values in the table are updated based on voted budget. As such, the last two bullets in the last paragraph are removed and the allocation of resources table is as follows:

2019	Total ABB budget (€)	Total ABB posts (FTEs)
Activity 1 - Expertise. Anticipate and support Europe in facing emerging network and information security challenges	3.732.004,50	11,51
Activity 2 - Policy. Promote network and information security an EU policy priority	4.904.920,21	27,45
Activity 3 - Capacity. Support Europe in maintaining state-of-the-art network and information security capacities	2.281.854,18	11,81
Activity 4 - Community. Foster the emerging European Network and Information Security Community	2.772.346,20	11,81
Activity 5 - Enabling. Reinforce ENISA's impact	3.241.826,95	35,42
Total	**16.932.952,05**	**98,00**

(b) Annex II. The tables following tables are replaced: Table 1 Expenditure overview, Commitment appropriations and Payments appropriations, Table 2. Revenue overview and Commitment appropriations and Payments appropriations as well as Table 3 — Budget out-turn and cancellation of appropriations. Calculation of budget out-turn. The new values are based on the voted 2019 budget.

The new text and tables are:

" A.2 Annex II: Human and financial resources 2019-2021

Table 1. Expenditure overview.

Expenditure	2018		2019		2020		2021	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1	6.386.500,00	6.386.500,00	9.387.948,32	9.387.948,32	12.038.000,00	12.038.000,00	13.343.500,00	13.343.500,00
Title 2	1.687.500,00	1.687.500,00	2.677.000,00	2.677.000,00	2.886.000,00	2.886.000,00	3.114.000,00	3.114.000,00
Title 3	3.354.126,00	3.354.126,00	4.868.003,73	4.868.003,73	6.858.958,98	6.858.958,98	6.968.901,60	6.968.901,60
Total expenditure	**11.428.126,00**	**11.428.126,00**	**16.932.952,05**	**16.932.952,05**	**21.782.958,98**	**21.782.958,98**	**23.426.401,60**	**23.426.401,60**

The tables below show the commitments and payment appropriations based on the same structure for the next years.

Commitment appropriations

EXPENDITURE	Executed budget 2017	Budget 2018	Envisaged in 2019	VAR 2019 / 2018	Envisaged in 2020	Envisaged in 2021	Envisaged in 2022
Title 1. Staff Expenditure	6.398.429,21	6.386.500,00	9.387.948,32	147%	12.038.000,00	13.343.500,00	13.875.000,00
11 Staff in active employment	4.674.963,79	5.186.400,00	6.794.000,00	131%	10.181.000,00	11.295.000,00	11.763.000,00
- of which establishment plan posts							
- of which external personnel							
12 Recruitment expenditure	175.432,52	261.100,00	968.948,32	371%	445.000,00	342.000,00	277.000,00
13 Socio-medical services and training	169.988,95	190.000,00	325.000,00	171%	250.000,00	305.000,00	375.000,00
14 Temporary assistance	1.378.043,95	749.000,00	1.300.000,00	174%	1.162.000,00	1.401.500,00	1.460.000,00
Title 2. Building, equipment and miscellaneous expenditure	1.600.312,46	1.687.500,00	2.677.000,00	159%	2.886.000,00	3.114.000,00	3.205.000,00
20 Building and associated costs	868.135,15	1.000.500,00	1.100.000,00	110%	1.180.000,00	1.234.000,00	1.234.000,00
21 Movable property and associated costs	25.435,15	60.000,00	58.000,00	97%	99.000,00	99.000,00	99.000,00
22 Current administrative expenditure	83.026,87	62.000,00	104.000,00	168%	176.000,00	201.000,00	201.000,00
23 ICT	623.715,29	565.000,00	1.415.000,00	250%	1.431.000,00	1.580.000,00	1.671.000,00
Title 3. Operational expenditure	3.176.483,82	3.354.126,00	4.868.003,73	145%	6.858.958,98	6.968.901,60	7.128.645,10
30 Activities related to meetings and missions	943.054,94	715.000,00	1.043.323,68	146%	1.407.325,78	1.421.124,00	1.415.000,00
32 Horizontal operational activities	569.390,45	660.000,00	614.680,05	93%	1.001.633,20	1.048.777,60	1.138.645,10
36 Core operational activities	1.664.038,43	1.979.126,00	3.210.000,00	162%	4.450.000,00	4.499.000,00	4.575.000,00
TOTAL EXPENDITURE	**11.175.225,49**	**11.428.126,00**	**16.932.952,05**	**148%**	**21.782.958,98**	**23.426.401,60**	**24.208.645,10**

Payments appropriations

EXPENDITURE	Executed budget 2017	Budget 2018	Envisaged in 2019	VAR 2019 / 2018	Envisaged in 2020	Envisaged in 2021	Envisaged in 2022
Title 1. Staff Expenditure	6.398.429,21	6.386.500,00	9.387.948,32	147%	12.038.000,00	13.343.500,00	13.875.000,00
11 Staff in active employment	4.674.963,79	5.186.400,00	6.794.000,00	131%	10.181.000,00	11.295.000,00	11.763.000,00
- of which establishment plan posts							
- of which external personnel							
12 Recruitment expenditure	175.432,52	261.100,00	968.948,32	371%	445.000,00	342.000,00	277.000,00
13 Socio-medical services and training	169.988,95	190.000,00	325.000,00	171%	250.000,00	305.000,00	375.000,00
14 Temporary assistance	1.378.043,95	749.000,00	1.300.000,00	174%	1.162.000,00	1.401.500,00	1.460.000,00
Title 2. Building, equipment and miscellaneous expenditure	1.600.312,46	1.687.500,00	2.677.000,00	159%	2.886.000,00	3.114.000,00	3.205.000,00
20 Building and associated costs	868.135,15	1.000.500,00	1.100.000,00	110%	1.180.000,00	1.234.000,00	1.234.000,00
21 Movable property and associated costs	25.435,15	60.000,00	58.000,00	97%	99.000,00	99.000,00	99.000,00
22 Current administrative expenditure	83.026,87	62.000,00	104.000,00	168%	176.000,00	201.000,00	201.000,00
23 ICT	623.715,29	565.000,00	1.415.000,00	250%	1.431.000,00	1.580.000,00	1.671.000,00
Title 3. Operational expenditure	3.176.483,82	3.354.126,00	4.868.003,73	145%	6.858.958,98	6.968.901,60	7.128.645,10
30 Activities related to meetings and missions	943.054,94	715.000,00	1.043.323,68	146%	1.407.325,78	1.421.124,00	1.415.000,00
32 Horizontal operational activities	569.390,45	660.000,00	614.680,05	93%	1.001.633,20	1.048.777,60	1.138.645,10
36 Core operational activities	1.664.038,43	1.979.126,00	3.210.000,00	162%	4.450.000,00	4.499.000,00	4.575.000,00
TOTAL EXPENDITURE	**11.175.225,49**	**11.428.126,00**	**16.932.952,05**	**148%**	**21.782.958,98**	**23.426.401,60**	**24.208.645,10**

Table 2 — Revenue overview

Revenues	2017	2018	2019	2020	2021
	Revenues estimated by the agency	Revenues estimated by the agency	Revenues estimated by the agency	Revenues estimated by the agency	Revenues estimated by the agency
EU contribution	10.322.000	10.529.000	15.910.000,00	20.646.000,00	22.248.000,00
Other revenue	853.225	899.126	1.022.952,05	1.136.958,98	1.178.401,60
Total revenues	**11.175.225**	**11.428.126**	**16.932.952,05**	**21.782.958,98**	**23.426.401,60**

REVENUES	2017 Executed Budget	2018 Budget	2019 Agency request	2019 Budget Forecast	VAR 2019 / 2018	Envisaged 2020	Envisaged 2021
1 REVENUE FROM FEES AND CHARGES							
2. EU CONTRIBUTION	10.322.000,00	10.529.000,00	15.910.000,00	15.910.000,00	51%	20.646.000,00	22.248.000,00
of which Administrative (Title 1 and Title 2)							
of which Operational (Title 3)							
of which assigned revenues deriving from previous years' surpluses							
3 THIRD COUNTRIES CONTRIBUTION (incl. EFTA and Candidate countries)	252.977,00	248.626,00	382.952,05	382.952,05	54%	496.958,98	538.401,60
of which EFTA	252.977,00	248.626,00	382.952,05	382.952,05	54%	496.958,98	538.401,60
of which Candidate Countries							
4 OTHER CONTRIBUTIONS	566.261,74	640.000,00	640.000,00	640.000,00	0%	640.000,00	640.000,00
of which delegation agreement, ad hoc grants							
5 ADMINISTRATIVE OPERATIONS	33.986,75	10.500,00	0,00	0,00		0,00	0,00
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT							
7 CORRECTION OF BUDGETARY IMBALANCES							
TOTAL REVENUES	**11.175.225,49**	**11.428.126,00**	**16.932.952,05**	**16.932.952,05**	**48%**	**21.782.958,98**	**23.426.401,60**

Table 3 — Budget out-turn and cancellation of appropriations. Calculation of budget out-turn

Budget outturn	2015	2016	2017	2018
Revenue actually received (+)	10.069.280,00	11.034.366,00	11.223.387,00	11.572.995,00
Payments made (-)	-9.395.559,00	-9.860.776,00	-9.901.545,00	-10.345.736,00
Carry-over of appropriations (-)	-674.521,00	-1.176.717,00	-1.376.730,00	-1.348.657,00
Cancellation of appropriations carried over (+)	80.675,00	38.616,00	90.916,00	108.302,00
Adjustment for carry over of assigned revenue appropriations from previous year (+)	800,00	3.127,00	49.519,00	124.290,00
Exchange rate differences (+/-)	-278,00	-180,00	-12,00	-689,00
Adjustment for negative balance from previous year (-)				
Total	**80.397,00**	**38.436,00**	**85.535,00**	**110.505,00**

(c.) Annex III Human resources – Quantitative has minimum changes, as the previous 'Scenario 2' matches voted resources.

In 'Table 1 — Staff population and its evolution; overview of all categories of staff' and in 'Table 2 — Multiannual staff policy plan 2019-2021' the column for Scenario 1 is removed as well as the text referring to 'Scenario 2' from the column for 2019 staff population.

(d) Annex IV: Human resources — Qualitative, is updated to align with the new priorities of the agency.

In the section 'A. Recruitment policy', the subsection 'Statutory staff' new bullet is added under "Operational job family':

"Operational job family

- Junior officer/administrator job category (staff providing junior expertise in a specific field of knowledge): typically, these posts are filled by grades AD 5, FG IV 13.
- Officer/administrator job category (staff providing officer expertise in a specific field of knowledge): typically, these posts are filled by grades AD 6-AD 7, FG IV 14-18.

- Lead officer/administrator (staff providing top level expertise in a specific field of knowledge): typically, these posts are filled by grades AD 8-AD 9.
- Team leader job category (staff providing operational excellence with some managerial responsibilities): typically, these posts are filed by grades AD 7-AD 10, FG IV 14-18.
- **Lead expert/Advisor job category (staff providing strategical operational excellence with some managerial responsibilities if needed): typically these posts are filled by grades AD9 – AD12.**"

In addition, where the contract length is described a new footnote is added to reflect the most recent updates, namely:

"**With the view to the draft CSA and with the aim to attract and retain the most qualified and motivated staff, the contract length for TA has been changed into 5 years initial contract with the possibility to be renewed for an indefinite period (ED Decision 16/2019 of 20 February 2019).**"

Section "C. Mobility policy" is updated with final 2018 information and the last paragraph is removed. This section is now:

"All internal moves are processed via Article 7 of the Staff Regulations and for transparency purposes are published internally on INTRAENISA. In order to create a motivated and versatile workforce, ENISA has adopted an ED policy 01/2017 of 22 February 2017 on internal mobility policy. ENISA also joined the inter-agency job market (IAJM) with the view, as for all other agencies, to offer possibilities of mobility to staff in agencies by assuring a continuation of careers and grades. In 2016 **and 2018**, **2**~~1~~ staff member**s** moved via the IAJM."

(e) Annex IX: Procurement plan 2019 is updated to reflect the new voted budget.

The new table summarizing the 2019 procurement plan is:

2019 WP Procurement Planning	**Direct budget (in EUR)**	**Procurement (tender) procedure required**	**Launch Dates**	**All other expenditure**
Activity 1 - Expertise. Anticipate and support Europe in facing emerging network and information security challenges	875.000,00	765.000,00	Q1-Q4	110.000,00
Activity 2 - Policy. Promote network and information security an EU policy priority	1.150.000,00	1.130.000,00	Q1-Q4	20.000,00
Activity 3 - Capacity. Support Europe in maintaining state-of-the-art network and information security capacities	535.000,00	505.000,00	Q1-Q4	30.000,00
Activity 4 - Community. Foster the emerging European Network and Information Security Community	650.000,00	580.000,00	Q1-Q4	70.000,00
Activity 5 - Enabling. Reinforce ENISA's impact	760.073,73	712.767,00	Q1-Q4	47.306,73
Total A1-A5	**3.970.073,73**	**3.692.767,00**	**Q1-Q4**	**277.306,73**

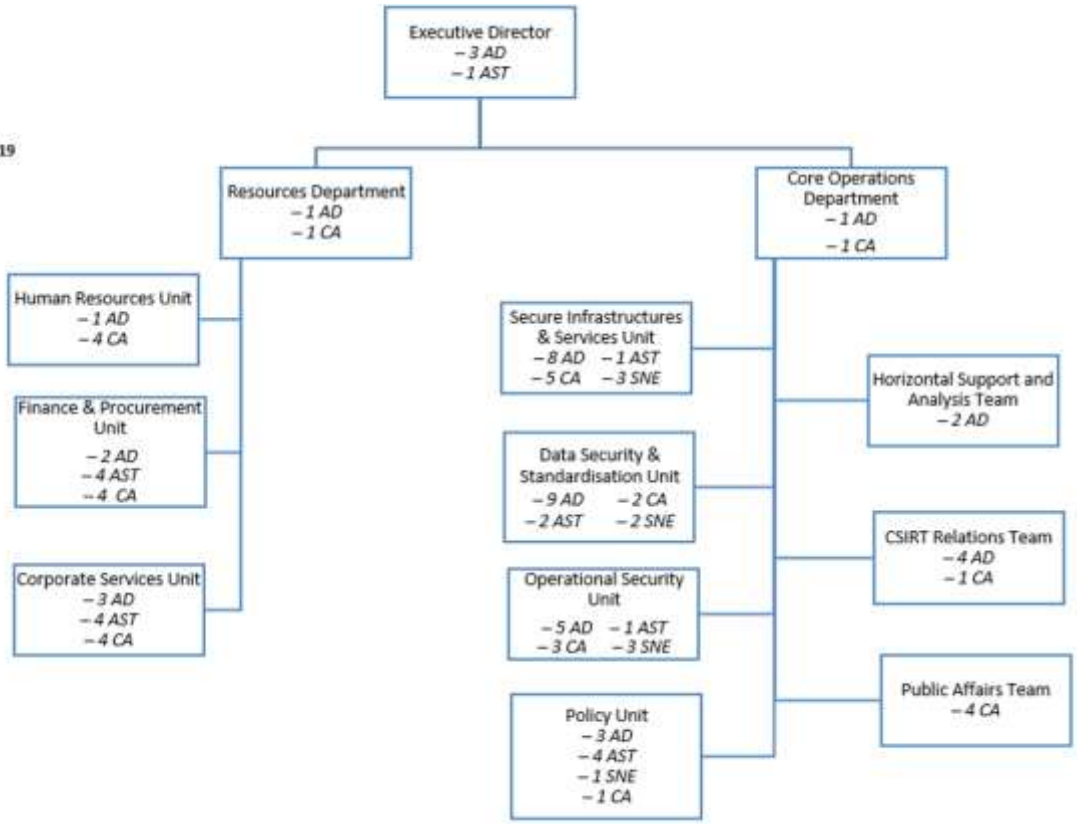
(f) Annex X: ENISA organisation is updated.

The text before the chart is removed, except "ENISA's organisation is presented below in detail." and the new organisation chart is:

Total

AD: 42
AST: 17
CA: 30
SNE: 9

Status of 1.03.2019



Statement of Estimates 2019 (Budget 2019)

European Union Agency for Network and Information Security

CONTENTS

1. General introduction
2. Justification of main headings
3. Statement of Revenue 2019
4. Statement of Expenditure 2019

1. GENERAL INTRODUCTION

Explanatory statement

Legal Basis:

1. Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013, concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) 460/2004.

Reference acts

Proposal for a Regulation of the European Parliament and of the Council, submitted by the Commission on 13 September 2017, on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) No 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act') (COM(2017) 477 final)

2. Financial Regulation of ENISA, adopted by the Management Board on 07 February 2014.

2. JUSTIFICATION OF MAIN HEADINGS

2.1 Revenue in 2019

The 2019 total revenue amounts to € 15910000 and consists of a subsidy from the General Budget of the European Commission, EFTA countries' contributions, € 382952,05 a subsidy from the Greek Government for the rent of the offices of ENISA in Greece €640000 and the interest on cash deposits.

2.2 Expenditure in 2019

The total forecasted expenditure is in balance with the total forecasted revenue.

Title 1 - Staff

The estimate of Title 1 costs is based on the Establishment Plan for 2019, which contains 59 Temporary Agent posts.

Total expenditure under Title 1 amounts to **€9.387.948,32**

Title 2 - Buildings, equipment and miscellaneous operating expenditure

Total expenditure under Title 2 amounts to **€2.677.000,00**

(including € 640.000,00 for the rent of two offices in Greece, subsidised by the Greek Government)

Title 3 - Operational expenditure

Operational expenditure is mainly related to the implementation of Work Programme 2019 and amounts to **€4.868.003,73**

3. STATEMENT OF REVENUE 2019

Title	Heading	Appropriations 2017 in €	Voted Appropriations 2018 in €	Voted Appropriations 2019 in €	Remarks - budget 2019
1	EUROPEAN COMMUNITIES SUBSIDY	10.322.000,00	10.529.000,00	15.910.000,00	Total subsidy of the European Communities
2	THIRD COUNTRIES CONTRIBUTION	252.977,00	248.626,00	382.952,05	Contributions from Third Countries.
3	OTHER CONTRIBUTIONS	566.261,74	640.000,00	640.000,00	Subsidy from the Government of Greece
4	ADMINISTRATIVE OPERATIONS	33.986,75	10.500,00	0,00	Other expected income.
	GRAND TOTAL	**11.175.225,49**	**11.428.126,00**	**16.932.952,05**	

Article Item	Heading	Appropriations 2017 in €	Voted Appropriations 2018 in €	Voted Appropriations 2019 in €	Remarks - budget 2019
1	EUROPEAN COMMUNITIES SUBSIDY				
10	EUROPEAN COMMUNITIES SUBSIDY				
100	*European Communities subsidy*	10.322.000,00	10.529.000,00	15.910.000,00	Regulation (EU) N° 526/2013 establishing an European Union Agency for Network and Information Security.
	CHAPTER 10	10.322.000,00	10.529.000,00	15.910.000,00	
	TITLE 1	10.322.000,00	10.529.000,00	15.910.000,00	
2	THIRD COUNTRIES CONTRIBUTION				
20	THIRD COUNTRIES CONTRIBUTION				
200	*Third Countries contribution*	252.977,00	248.626,00	382.952,05	Contributions from Associated Countries.
	CHAPTER 2 0	252.977,00	248.626,00	382.952,05	
	TITLE 2	252.977,00	248.626,00	382.952,05	
3	OTHER CONTRIBUTIONS				
30	OTHER CONTRIBUTIONS				
300	*Subsidy from the Ministry of Transports of Greece*	566.261,74	640.000,00	640.000,00	Subsidy from the Government of Greece.
	CHAPTER 30	566.261,74	640.000,00	640.000,00	
	TITLE 3	566.261,74	640.000,00	640.000,00	
4	ADMINISTRATIVE OPERATIONS				
40	ADMINISTRATIVE OPERATIONS				
400	*Administrative Operations*	33.986,75	10.500,00	0,00	Revenue from administrative operations.
	CHAPTER 40	33.986,75	10.500,00	0,00	
	TITLE 4	33.986,75	10.500,00	0,00	
	GRAND TOTAL	11.175.225,49	11.428.126,00	16.932.952,05	

4. STATEMENT OF EXPENDITURE 2019

Title	Heading	Appropriations 2017 in €	Voted Appropriations 2018 in €	Voted Appropriations 2019 in €	Remarks - budget 2019
1	STAFF	6.398.429,21	6.386.500,00	9.387.948,32	Total funding for covering personnel costs.
2	BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE	1.600.312,46	1.687.500,00	2.677.000,00	Total funding for covering general administrative costs.
3	OPERATIONAL EXPENDITURE	3.176.483,82	3.354.126,00	4.868.003,73	Total funding for operational expenditures.
	GRAND TOTAL	11.175.225,49	11.428.126,00	16.932.952,05	

1	STAFF				
11	STAFF IN ACTIVE EMPLOYMENT				
110	*Staff holding a post provided for in the establishment plan*				
1100	Basic salaries	3.406.541,98	3.779.100,00	5.000.000,00	Staff Regulations applicable to officials of the European Communities, and in particular Articles 62 and 66 thereof. This appropriation is intended to cover salaries, allowances, and employee contributions on salaries of permanent officials and Temporary Agents (TA), as of 2016

1101	Family allowances	p.m.	p.m.	p.m.	Staff Regulations applicable to officials of the European Communities, and in particular Articles 62, 67 and 68 thereof and Section I of Annex VII thereto. This appropriation is intended to cover the household, dependent child and education allowances which will be reported in items 1100 (for TA) and 1110 (for CA) since year 2016.
1102	Expatriation and foreign-residence allowances	p.m.	p.m.	p.m.	Staff Regulations applicable to officials of the European Communities, and in particular Articles 62 and 69 thereof and Article 4 of Annex VII thereto. This appropriation is intended to cover the expatriation and foreign-residence allowances which will be reported in items 1100 (for TA) and 1110 (for CA) since year 2016.
	Article 1 1 0	3.406.541,98	3.779.100,00	5.000.000,00	
111	***Other staff***				
1110	Contract Agents	1.177.078,03	1.168.300,00	1.650.000,00	Conditions of employment of other servants of the European Communities, and in particular Article 3 and Title III thereof. This appropriation is intended to cover salaries, allowances, and employee contributions on salaries of Contract Agents (CA), as of 2016
1113	Seconded National Experts (SNEs)	91.343,78	239.000,00	144.000,00	To cover basic salaries and all benefits of SNEs.
	Article 111	1.268.421,81	1.407.300,00	1.794.000,00	
112	***Employer's Social Security Contributions***				
1120	Insurance Against Sickness	p.m.	p.m.	p.m.	Staff Regulations applicable to officials of the European Communities, and in particular Article 72 thereof. Rules on sickness insurance for officials of the European Communities, and in particular Article 23 thereof. This appropriation is intended to cover sickness insurance costs which will be reported in items 1100 (for TA) and 1110 (for CA) since year 2016.
1121	Insurance Against Occupational Disease and Accidents	p.m.	p.m.	p.m.	Staff Regulations applicable to officials of the European Communities, and in particular Article 73 thereof. This appropriation is intended to cover the employer's contribution to insurance against accidents and occupational diseases which will be reported in items 1100 (for TA) and 1110 (for CA) since year 2016.
1122	Insurance Against Unemployment	p.m.	p.m.	p.m.	Council Regulation (ECSC, EEC, Euratom) No 2799/85 of 27 September 1985 amending the Staff Regulations of officials and the conditions of employment of other servants of the European Communities (OJ L 265, 8.10.1985, p. 1). This appropriation is intended to cover the costs of insurance against unemployment which will be reported in items 1100 (for TA) and 1110 (for CA) since year 2016.
	Article 1 1 2	0,00	0,00	0,00	
113	***Miscellaneous Allowances and Grants***				
1130	Childbirth and Death Allowances and Grants	p.m.	p.m.	p.m.	Staff Regulations applicable to officials of the European Communities, and in particular Articles 70, 74 and 75 thereof. This item is intended to cover the childbirth grant and, in the event of the death of an official, payment of the deceased's full remuneration which will be reported in items 1100 (for TA) and 1110 (for CA) since year 2016.
1131	Annual Travel Expenses from the Place of Work to Origin	p.m.	p.m.	p.m.	Staff Regulations applicable to officials of the European Communities, and in particular Article 8 of Annex VII thereto. This appropriation is intended to cover the flat-rate travel expenses for officials or temporary staff, their spouses and dependants which will be reported in items 1100 (for TA) and 1110 (for CA) since year 2016.
	Article 1 1 3	0,00	0,00	0,00	
119	***Salary Weightings***				
1190	Salary Weightings	p.m.	p.m.	p.m.	Staff Regulations applicable to officials of the European Communities, and in particular Articles 64 and 65 thereof. This appropriation is intended to cover the impact of salary weightings applicable to the remuneration of officials and temporary staff.
	Article 1 1 9	p.m.	p.m.	p.m.	
	CHAPTER 11	**4.674.963,79**	**5.186.400,00**	**6.794.000,00**	

12	**RECRUITMENT EXPENDITURE**				
120	***Travel Expenses in interviewing candidates***				
1200	Travel Expenses in interviewing candidates	31.368,58	19.000,00	97.000,00	This appropriation is to cover travel expenditures incurred for interviewing candidates.
	Article 1 2 0	31.368,58	19.000,00	97.000,00	
121	***Expenditure on entering/leaving and transfer***				
1210	Expenses on Taking Up Duty and on End of Contract	7.519,11	9.600,00	40.000,00	Staff Regulations applicable to officials of the European Communities, and in particular Articles 20 and 71 thereof and Article 7 of Annex VII thereto. This appropriation is intended to cover the travel expenses of staff (including members of their families).
1211	Installation, Resettlement and Transfer Allowance	22.723,68	68.000,00	356.042,32	Staff Regulations applicable to officials of the European Communities, and in particular Articles 5 and 6 of Annex VII thereto. This appropriation is intended to cover the installation allowances for staff obliged to change residence after taking up their duty.
1212	Removal Expenses	74.344,35	68.000,00	247.000,00	Staff Regulations applicable to officials of the European Communities, and in particular Articles 20 and 71 thereof and Article 9 of Annex VII thereto. This appropriation is intended to cover the removal costs of staff obliged to change residence after taking up duty.
1213	Daily Subsistence Allowance	39.476,80	96.500,00	228.906,00	Staff Regulations applicable to officials of the European Communities, and in particular Articles 20 and 71 thereof and Article 10 of Annex VII thereto, as well as Articles 25 and 67 of the Conditions of Employment of other Servants. This appropriation is to cover the costs of daily subsistance allowances.
	Article 1 2 1	144.063,94	242.100,00	871.948,32	
	CHAPTER 1 2	**175.432,52**	**261.100,00**	**968.948,32**	
13	**SOCIO-MEDICAL SERVICES AND TRAINING**				
131	***Medical Service***				
1310	Medical Service	27.755,86	35.000,00	75.000,00	This appropriation is intended to cover the costs of annual medical inspections and of reviewing the health and safety at work conditions.
	Aticle 1 3 1	27.755,86	35.000,00	75.000,00	
132	***Training***				
1320	Language Courses and Other Training	142.233,09	155.000,00	250.000,00	This appropriation is intended to cover the costs of language and other training needs.
	Article 1 3 2	142.233,09	155.000,00	250.000,00	
	CHAPTER 1 3	**169.988,95**	**190.000,00**	**325.000,00**	
14	**TEMPORARY ASSISTANCE**				
140	***European Commission Management Costs***				
1400	EC Management Costs	40.020,13	54.000,00	58.000,00	This appropriation is intended to cover the costs of the EC management costs.
	Article 1 4 0	40.020,13	54.000,00	58.000,00	
141	***Social welfare***				
1410	Special Assistance Grants	0,00	0,00	0,00	This appropriation is intended to cover special assistance grants.
1411	Other welfare expenditure	127.043,30	130.000,00	110.000,00	This appropriation is intended to cover other welfare expenditure.
1412	Schooling & Education expenditure	307.071,16	300.000,00	420.000,00	This appropriation is intended to cover the subsidy for the functioning of the School of European Education of Heraklion, and other expenditure relevant to schooling & education of children of the Agency staff.
	Article 1 4 1	434.114,46	430.000,00	530.000,00	

142	***Temporary Assistance***				
1420	Interim Service	733.793,22	155.000,00	572.000,00	This appropriation is intended to cover the costs of temporary assistance.
1421	Consultants	170.116,14	95.000,00	115.000,00	This appropriation is intended to cover expenditure of contracting consultants.
1422	Internal Control and Audit	0,00	15.000,00	25.000,00	This appropriation is intended to cover expenditure related to the development and functioning of Internal Audit Capability (IAC) and Internal Control Coordination functions.
	Article 1 4 2	903.909,36	265.000,00	712.000,00	
	CHAPTER 1 4	**1.378.043,95**	**749.000,00**	**1.300.000,00**	
	Total Title 1	**6.398.429,21**	**6.386.500,00**	**9.387.948,32**	
2	**BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE**				
20	**BUILDINGS AND ASSOCIATED COSTS**				
200	**Buildings and associated costs**				
2000	Rent of buildings	566.261,74	640.000,00	640.000,00	This appropriation is intended to cover the payment of rents for buildings or parts of buildings occupied by the Agency and the hiring of parking spaces.
2002	Building Insurance	1.823,12	5.500,00	6.000,00	This appropriatio id intended to cover the insurance costs of the premises of the Agency.
2003	Water, gas, electricity and heating	47.771,74	85.000,00	130.000,00	This appropriation is intended to cover the costs of utitlities for the premises of the Agency.
2004	Cleaning and maintenance	59.207,63	55.000,00	74.000,00	This appropriation is intended to cover the costs of cleaning and upkeeping of the premises used by the Agency.
2005	Fixtures and Fittings	18.650,26	15.000,00	25.000,00	This appropriation is intended to cover the fitting-out of the premises and repairs in the building.
2006	Security equipment	613,67	15.000,00	25.000,00	This appropriation is intended to cover purchases and maintenance cost of equipment related to security and safety of the building and the staff.
2007	Security Services	81.387,94	110.000,00	140.000,00	This appropriation is intended to cover expenditure on buildings connected with security and safety, in particular contracts governing building surveillance.
2008	Other expenditure on buildings	92.419,05	75.000,00	60.000,00	The appropriation is intended to cover expenditure on buildings not specially provided for in the articles in Chapter 20, for example market survey costs for rent of buildings, and costs of departmental removals and other handling costs.
	Article 2 0 0	868.135,15	1.000.500,00	1.100.000,00	
	CHAPTER 2 0	**868.135,15**	**1.000.500,00**	**1.100.000,00**	
21	**MOVABLE PROPERTY AND ASSOCIATED COSTS**				
210	***Technical Equipment and installations***				
2100	Technical Equipment and services	1.810,40	15.000,00	25.000,00	This appropriation is intended to cover expenditure of acquiring technical equipment, as well as maintenance and services related to it.
	Article 2 1 0	1.810,40	15.000,00	25.000,00	
211	***Furniture***				
2110	Furniture	11.566,17	30.000,00	15.000,00	This appropriation is to cover the costs of purchasing, leasing, and repairs of furniture.
	Article 2 1 1	11.566,17	30.000,00	15.000,00	
212	***Transport Equipment***				
2120	Transport Equipment	p.m.	p.m.	p.m.	This appropriation is to cover the costs of purchasing and leasing of transport equipment.
2121	Maintenance and Repairs of transport equipment	9.294,58	10.000,00	12.000,00	This appropriation is to cover the costs of maintenance and repairs of transport equipment as well as insurance and fuel.
	Article 2 1 2	9.294,58	10.000,00	12.000,00	

213	***Library and Press***				
2130	Books, Newspapers and Periodicals	2.764,00	5.000,00	6.000,00	This appropriation is intended to cover the purchase of publications and subscriptions to information services necessary for the work of the Agency, including books and other publications, newspapers, periodicals, official journals and subscriptions.
	Article 2 1 3	2.764,00	5.000,00	6.000,00	
	CHAPTER 2 1	**25.435,15**	**60.000,00**	**58.000,00**	
22	**CURRENT ADMINISTRATIVE EXPENDITURE**				
220	***Stationery, postal and telecomunications***				
2200	Stationery	47.047,69	30.000,00	60.000,00	This appropriation is intended to cover the costs of office stationery.
2201	Postage and delivery charges	21.000,00	19.000,00	20.000,00	This appropriation is intented to cover post office and special courrier costs.
2203	Other Office Supplies	13.979,18	12.000,00	23.000,00	This appropriation is intended to cover the purchase of various office supplies.
	Article 2 2 0	82.026,87	61.000,00	103.000,00	
221	***Financial charges***				
2210	Bank charges and interest paid	1.000,00	1.000,00	1.000,00	This appropriation is intended to cover bank charges, interest paid and other financial and banking costs.
	Article 2 2 1	1.000,00	1.000,00	1.000,00	
223	***Damages***				
2230	Damages	p.m.	p.m.	p.m.	This appropriation is intended to cover the costs of damages to the Agency.
	Article 2 2 3	p.m.	p.m.	p.m.	
	CHAPTER 2 2	**83.026,87**	**62.000,00**	**104.000,00**	
23	**ICT**				
230	***ICT***				
2304	Service Transition	200.646,90	130.000,00	600.000,00	This appropriation is intended to cover the costs of purchasing hardware & software, as well as maintenance and consultancy services related to the transition to new ICT infrastructure and systems.
2305	Service Operations	110.231,20	95.000,00	220.000,00	This appropriation is intended to cover the costs of purchasing hardware & software, as well as maintenance and consultancy services related to existing ICT operations
2306	Service Security	p.m.	p.m.	p.m.	This appropriation is intended to cover the costs of purchasing hardware & software, as well as maintenance and consultancy services related to the ICT security layer
2307	Service External	312.837,19	340.000,00	595.000,00	This appropriation is intended to cover the costs of outsourced services, including hosting, telecommunications, ISP, subscriptions and investment in new tools
2308	Service Strategy	p.m.	p.m.	p.m.	This appropriation is intended to cover the costs related to strategy definition and strategic planning.
	Article 2 3 0	623.715,29	565.000,00	1.415.000,00	
	CHAPTER 2 3	**623.715,29**	**565.000,00**	**1.415.000,00**	
	Total Title 2	**1.600.312,46**	**1.687.500,00**	**2.677.000,00**	
3	**OPERATIONAL EXPENDITURE**				
30	**ACTIVITIES RELATED TO MEETINGS AND MISSIONS**				
300	***Meetings of the Bodies of the Agency***				
3001	Meetings of Official Bodies	81.554,94	120.000,00	**120.000,00**	This appropriation is intended to cover the costs of meetings of the official bodies of the Agency, i.e. Management Board and National Liaison officers network meetings, including travel costs of experts participating. As of 2017, the PSG meetings are funded from item 3200.
3005	Executive Director Office Meetings	p.m.	p.m.	p.m.	This appropriation is intended to cover the costs of the Executive Director Office meetings, including travel costs of experts participating in group meetings.
	Article 3 0 0	81.554,94	120.000,00	120.000,00	
301	***Mission and Representation Costs***				
3011	Entertainment and Representation expenses	4.000,00	2.500,00	15.393,68	This appropriation is intended to cover the costs of entertainment and representation expenses.
3016	Missions	852.500,00	590.000,00	897.930,00	This appropriation is intended to cover the costs of all staff and SNE mission related costs.
	Article 3 0 1	856.500,00	592.500,00	913.323,68	

302	***Other meetings***				
3021	Other Operational meetings	5.000,00	2.500,00	10.000,00	This appropriation is intended to cover the costs of the various operational meetings.
	Article 3 0 2	5.000,00	2.500,00	10.000,00	
	CHAPTER 3 0	**943.054,94**	**715.000,00**	**1.043.323,68**	
32	**HORIZONTAL OPERATIONAL ACTIVITIES**				
320	***Conferences and Joint Events***				
3200	Horizontal Operational meetings	272.159,31	165.000,00	214.608,05	This appropriation is intended to cover the costs of horizontal operational meetings, including the costs of Permanent Stakeholders' Group (PSG) meetings and relevant travel costs. As from 2019 II half the cost of the NLO meetings are covered under item 3001
	Article 3 2 0	272.159,31	165.000,00	214.608,05	
321	***Communication and Information dissemination***				
3210	Communication activities	48.234,00	80.000,00	150.000,00	This appropriation is intended to cover the costs of the Corporate communication activities and the activities of the Spokesperson of the Agency.
3211	Internal Communication	59.698,41	20.000,00	0,00	This appropriation is intended to cover the costs of internal communication activities of the Agency.
3212	Stakeholders' communication	113.908,71	160.000,00	113.000,00	This appropriation is intended to cover the costs of activities related to communication with Stakeholders of the Agency.
	Article 3 2 1	221.841,12	260.000,00	263.000,00	
322	***Web-Site Development***				
3220	Web-Site Development	p.m.	p.m.	p.m.	This appropriation is intended to cover the costs of further developing and mainting the main web pages of the Agency.
	Article 3 2 2	0,00	0,00	0,00	
323	***Translation and interpretation services***				
3230	Translations	20.500,00	15.000,00	30.072,00	This appropriation is intended to cover the costs of translations of documents for the Agency.
	Article 3 2 3	20.500,00	15.000,00	30.072,00	
324	***Publications***				
3240	Publications	0,00	0,00	0,00	This appropriation is intended to cover the costs of publications of the Agency, other than deliverables or communication material.
	Article 3 2 4	0,00	0,00	0,00	
325	***Operational Systems***				
3250	Operational Systems	39.890,02	80.000,00	57.000,00	This appropriation is intended to cover the costs of development and hosting of external facing systems, e.g. ENISA website
	Article 3 2 5	39.890,02	80.000,00	57.000,00	
326	***Strategy and Evaluation***				
3260	*Strategic consultancy*	15.000,00	40.000,00	50.000,00	This appropriation is intended to cover the costs of consultancy services related to the strategy of the Agency.
3261	*External Evaluations*	p.m.	100.000,00	0,00	This appropriation is intended to cover the costs of external evaluations of the Agency activities.
	Article 3 2 6	15.000,00	140.000,00	50.000,00	
	CHAPTER 3 2	**569.390,45**	**660.000,00**	**614.680,05**	

36	**CORE OPERATIONAL ACTIVITIES**					
360	***Stakeholders' collaboration***					
3600	Stakeholders' collaboration		p.m.	p.m.	p.m.	This appropriation is intended to cover the costs of activities related to support of CERT operation and cooperation, as well as stakeholders' collaboration activities, including cooperation of communities that deal with improving pan-European or international NIS.
		Article 3 6 0	0,00	0,00	0,00	
361	***NIS Policy***					
3610	NIS Policy		p.m.	p.m.	p.m.	This appropriation is intended to cover the costs of activities related to development of policies and practices, that will contribute to strenghtening pan-European CIIP and Resilience
		Article 3 6 1	0,00	0,00	0,00	
362	***NIS Technology***					
3620	NIS Technology		p.m.	p.m.	p.m.	This appropriation is intended to cover the costs of activities related to developments in the area of NIS Technology.
		Article 3 6 2	0,00	0,00	0,00	
363	***Activity: Expertise***					
3630	Activity: Expertise		427.962,94	536.626,00	875.000,00	This appropriation is intended to cover the costs of Activity 1 – Expertise. Anticipate and support Europe in facing emerging network and information security challenges
		Article 3 6 3	427.962,94	536.626,00	875.000,00	
364	***Activity: Policy***					
3640	Activity: Policy		541.664,06	646.500,00	1.150.000,00	This appropriation is intended to cover the costs of Activity 2 – Policy. Make network and information security an EU policy priority
		Article 3 6 4	541.664,06	646.500,00	1.150.000,00	
365	***Activity: Capacity***					
3650	Activity: Capacity		368.196,36	300.000,00	535.000,00	This appropriation is intended to cover the costs of Activity 3 – Capacity. Support Europe in setting up state-of-the-art network and information security capacities
		Article 3 6 5	368.196,36	300.000,00	535.000,00	
366	***Activity: Community***					
3660	Activity: Community		326.215,07	496.000,00	650.000,00	This appropriation is intended to cover the costs of Activity 4 – Community. Make the European network and information security community a reality
		Article 3 6 6	326.215,07	496.000,00	650.000,00	
		CHAPTER 3 6	**1.664.038,43**	**1.979.126,00**	**3.210.000,00**	
		TITLE 3	**3.176.483,82**	**3.354.126,00**	**4.868.003,73**	
		GRAND TOTAL	**11.175.225,49**	**11.428.126,00**	**16.932.952,05**	